OPINION ISSUED IN PLENARY TO BILL NO. 2.630, OF 2020, AND APPENDED BILLS

BILL NO. 2.630, OF 2020

(Attached Bills - PL nos 3063/2020, PL 3144/2020, PL 3627/2020, PL 1676/2015, PL 2712/2015, PL 346/2019, PL 283/2020, PL 2854/2020, PL 3029/2020 , PL 2883/2020, PL 649/2021, PL 3119/2020, PL 1589/2021, PL 2393/2021, PL 2831/2021, PL 3395/2020, PL 291/2021, PL 449/2021, PL 3700/2021, PL 3573/2020, PL 213/2021, PL 495/2021, PL 2401/2021, PL 127/2021, PL 246/2021, PL 1362/2021, PL 865/2021, PL 2390/2021, PL 10860/2018, PL 5776/2019, PL 475/2020, PL 4418/2020, PL 1743/2021, PL 3389/2019, PL 4925/2019, PL 5260/2019, PL 437/2020, PL 2284/2020, PL 6351/2019, PL 517/2020, PL 3044/2020, PL 1590/2021, PL 2989/2021, PL 2763/2020, PL 6812/2017, PL 7604/2017, PL 9647/2018, PL 2601/2019, PL 2602/2019, PL 8592/2017, PL 9554/2018, PL 9554/2018, PL 9533/2018, PL 9761/2018, PL 9838/2018, PL 9884/2018, PL 9931/2018, PL 4134/2021, PL 200/2019, PL 241/2019, PL 3307/2020, PL 693/2020, PL 705/2020, PL 1394/2020, PL 988/2020, PL 1923/2021, PL 1258/2020, PL 1941/2020, PL 2389/2020, PL 2790/2020, PL 1001/2021, PL 2196/2020, PL 1897/2021, PL 3857/2019, PL 1974/2019, PL 2844/2020, PL 3222/2020, PL 356/2021, PL 388/2021, PL 5959/2019, PL 1772/2021, PL 2060/2021, PL 3366/2021, PL 143/2022, PL 714/2022, PL 836/2022; PL 2516/2022; PL 125/2023; PL 1087/2023; PL 1116/2023)

Establishes the Brazilian Law of Freedom, Responsibility and Transparency on the Internet.

Autor: SENATE FEDERAL; Senator ALESSANDRO VIEIRA

Rapporteur: Deputy ORLANDO SILVA

I - REPORT

This Plenary examines Bill no. 2630 of 2020, authored by Senator Alessandro Vieira, to regulate transparency rules for social network providers and private messaging services, in order to ensure security and ample freedom of expression, communication, and expression of thought.

In Chapter I, the proposal establishes the principles by which the law will be guided, including, for example, the principle of transparency in the rules for the broadcasting of ads and paid content. Next, it outlines the objectives of the law, highlighting the strengthening of the

democratic process, the defense of freedom of expression, and the prevention of censorship in the environment

online, the search for greater transparency in moderation practices of content posted by third parties on social networks, and the adoption of mechanisms and tools to provide information about boosted and advertising content made available to the user. At the end, the chapter provides the relevant definitions that will be used in the application of the law.

In Chapter II, the bill establishes general and specific rules for accountability and transparency in the use of social networking and private messaging services. Among the general rules, the bill prohibits the operation of inauthentic accounts and automated accounts that are not identified as such, and provides for the possibility of requiring confirmation of identification of users and those responsible for the accounts. There is also provision for the adoption of moderation procedures, ensuring users the right to compensation for individual or collective damage to fundamental rights and the right to appeal the unavailability of content and accounts.

Specifically for private messaging services, there is provision to limit the number of forwardings of the same message to users or groups, and for prior user consent for inclusion in messaging groups. For social network providers there are obligations, for example, to produce quarterly transparency reports and to identify all promoted and advertising content.

In Chapter III, the proposal addresses the actions of public authorities, regulating the social network accounts used by direct or indirect public administration entities and bodies and by political agents, as well as determining transparency rules for data on the contracting of advertising and publicity services or content boosting via the internet.

Chapter IV provides for the creation of an Internet Transparency and Accountability Council, which will be responsible for conducting studies, opinions and recommendations on Internet freedom, accountability and transparency. The Council will be responsible, among other competencies, for elaborating a code of conduct for social networks and private messaging services, to be evaluated and approved by the National Congress, for evaluating the adequacy of the usage policies adopted by social network providers and private messaging services, and for evaluating the moderation procedures adopted by social network providers, as well as suggesting guidelines for their implementation.

Chapter V contains rules for regulated self-regulation, providing that providers of social networking and private messaging services may create a self-regulatory institution focused on transparency and accountability in Internet use. The goal, among others, is to improve rules and procedures for deciding on the adoption of informative measures and the provision of an efficient service for the forwarding of complaints. Chapter VI provides for sanctions to be applied by the Judiciary in cases of non-compliance with the law, foreseeing penalties of a warning, with an indication of the deadline for the adoption of corrective measures, and a fine of up to 10% of the income of the economic group in Brazil in its last year.

In the final provisions, contained in Chapter VII, the bill introduces the obligation to appoint legal representatives in Brazil for providers of social networks and private messaging services, creates new requirements for the formation of a pre-paid telephone register, and new hypotheses of administrative improbity against the principles of public administration.

Also in 2020, the Cycle of Public Debates was held to discuss the PL nº 2.630/2020, which institutes the Brazilian Law of Freedom, Responsibility and Transparency on the Internet, with eleven discussion tables and the participation of 72 specialists and numerous and active participation of Internet users through e-Democracy. We will present below a summary of the main issues discussed in the Cycle and, at the end, a summary of each of the roundtables.

Table 1 discussed the importance of a law to combat disinformation. There was consensus in its necessity for the Brazilian context, mainly due to inauthentic behaviors and the dissemination of false or distorted information, but without vigilantism and barriers to innovation. Roundtable 2 focused on the transparency of actions by platforms. There was agreement about the importance of publishing

reports containing the platforms' mediation actions. Table 3 discussed content moderation practices and, although there was harmony about the importance of knowledge and publication of the mechanisms used by apps, concerns were expressed about: excessive detailing of conditions in the law; increase in the dominant position of platforms; difficulties of implementation by small companies; and the wording of article 12. Table 4 focused on advertising and content boosting. Boosting was considered positive due to the cheapening of advertising campaigns, but there was criticism regarding the lack of accountability of platforms for the ads broadcasted, lack of regulatory symmetry with the other mass communication vehicles. The issue of the treatment of electoral content in that sphere was also raised. Table 5 discussed disinformation and its impact on democracy. Here there was a greater mosaic of positions, with conflicting opinions regarding self-regulation and the Congressional Council foreseen for monitoring the future law. There was consensus, however, on the slowness of justice and the danger that the traceability foreseen in art. 10 imposes on individual liberties. Table 6 focused on account identification procedures, and there was broad consensus that the possibility of document collection was disproportionate and ineffective. Table 7 discussed private messaging, and there was some unity in considering the guarding of metadata to be dangerous to privacy, as well as ineffective in identifying the originators of disinformation. Roundtable 8 addressed the implications of technology on national sovereignty, where concerns were expressed about the vulnerability created by centralizing data storage in the national territory only, and the difficulty of exercising sovereignty due to the global nature of the internet. Table 9 dealt with the financing of disinformation. There was agreement about the need to demonetize this "industry", which includes the participation of public agents, and disagreement about the need or not of new criminal types to curb this practice. Roundtable 10 dealt with the issue of media education, when the consensus was more generalized, and pointed out the need for greater detailing of possible educational actions and integration with the Common National Curricular Base. Roundtable 11, focused on the issue of hate speech, indicated the need for transparency in moderation processes, but without consensus about the best way.

On 04/15/2021, the proposal was distributed to the Committees of Science and Technology, Communication and Informatics, Finance and Taxation, and Constitution and Justice and Citizenship, the three of them to pronounce on the merit, the second also on the financial or budgetary adequacy and the third on the constitutionality or legality of the matter. The proposition is subject to Plenary Appreciation and follows the priority proceeding regime, under the terms of art. 151, II, of the Internal Rules of the House of Representatives.

There was also 1 meeting in the scope of the Science and Technology, Communications, and Information Technology Commission - CCTCI and 14 meetings in the scope of the Working Group, with a total of 15 public hearings, the content of which we will report below.

The 1st public hearing, which took place on 08/06/2021, in the scope of the working group, dealt with the topic "Regulatory Paths to Confront Disinformation". Ms. Ana Paula Bialer pointed out that it is important to translate foreign concepts to the Brazilian reality. To defocus the discussion from the platforms and focus on who does the misinformation. She defended that there are two paths, one more traditional, with prescriptive legislation and sanctioning structures, and the other less rigid, more collaborative or self-regulation. The latter has more positive results in an environment of great innovation, such as the internet. An example is the European code of conduct. Mr. Carlos Affonso Souza defended the possibility of application providers' moderation activity, which is important. Creating rules for moderation, prohibiting or restricting account suspensions can be problematic. He made comparisons with American legislation to say that, in Brazil, there is no immunity for moderation that is illegal, so it doesn't make sense to take away a non-existent right. The best would be to make it clear that moderation can be done, and that it must be transparent and effective. Ms. Clara Iglesias Keller - Coordinator of the Digital Disinformation Hub at the Leibniz Institute for Media Research - stressed the need for clarification of some concepts, such as disinformation and automated accounts. She said it is interesting to identify

issues concerning content regulation, advertising targeting, and tools to combat misinformation. Regulatory strategies should, according to her, move away from direct regulation of content and focus on transparency and monitoring of the law's obligations. Self-regulatory mechanisms may be opportune. Mr. Demi Getschko - Nic.br CEO - spoke about basic internet concepts, emphasizing that Brazil already has a legal framework for the internet and that care must be taken so that the legislation does not become obsolete quickly. Ms. Laura Moraes, Senior Advocacy Campaign Coordinator at AVAAZ, defended that the proposal should focus on legislation on users' rights. The goal should be more transparency and access to information, not content removal. There is a lack of clarity in the text about the enforcement powers established in the PL. The data should be available for us to know what happens inside the platforms and for researchers. Next, Ms. Raquel Saraiva highlighted art. 19 of the MCI, which discourages censorship in the virtual media. She argued for the adoption of clear criteria for content removal and editing for users, and also for transparency reports about the providers' activities for the general public. He defended that art. 10 of the Senate's text should be changed, as it implies in massive surveillance, relativizing the rights to privacy. Renata Mielli, Coordinator of the Alternative Media Study Center Barão de Itararé, spoke about the disinformation and the degradation of the public sphere of debate, and that the discussion should be guided by the attempt to improve this environment. It would be a mistake to regulate types of discourse or what the user can do, because it would be giving even more power to the big private technology companies. He pointed out that there is a greater consensus on transparency processes and less opacity, with periodic reporting obligations. Moderation is necessary, but the power cannot be indiscriminate and it would be good to create a due process of law for moderation. Mr. Renato Franco de Moraes said that the PL seems to place too much responsibility on ISPs. There are some norms in the PL that are not principled, such as the prohibition of inauthentic and automated accounts, which can cause problems. He opined that the MCI system for content removal, apart from user notification, works well. It would not be necessary to create an appeal instance within the provider itself, which would plaster the procedure and who will decide the point in the end will be the judge.

At the 2nd public hearing, held on 08/10/2021, with the theme "Transparency and Accountability Measures", Ms. Rebeca Garcia, Public Policy Manager at Facebook in Brazil, sustained that one should avoid the temptation of drafting a very restrictive proposal, which does not mean debating the possibility of regulation, but always with technological neutrality. He stressed that transparency is not an end in itself, but should remain useful as challenges change. Next, Ms. Ramênia Vieira, from Intervozes, defended the advance in transparency of platforms and accountability of these entities. Users should be fully aware of the moderation policies adopted, and platforms should be transparent about the curation mechanisms, when and how the algorithm affects users' expression. Mr. Thiago Rondon, Executive Director of the Civic App and Digital Coordinator of Combating Disinformation at the Superior Electoral Court (TSE), spoke about initiatives to combat fake news, such as the Coalition of Checks, among others. He highlighted that most of the population doesn't have access to data and these initiatives work in this sense. We must, he argued, avoid setbacks, and guarantee important achievements such as the right to cryptography and debate the responsibility for transparency in the public space about demonetization and content removal. Mr. José Renato Laranjeira, Director of the Laboratory of Public Policy and Internet - LAPIN, noted that automated data processing can lead to decision errors. Therefore, transparency must be guaranteed proportionally to the target audience. Transparency should differentiate which type of moderation was used and its impact and justifiability, and human bias should be maintained. Mr. Ricardo Campos, Director of the Institute Legal Grounds for Privacy Design - LGPD, said that we are moving towards a 2nd phase of the Internet, no longer having more horizontal relationships and moving towards more vertical and mediated relationships. About content moderation, he stated that the freedom of expression of those who are inside private platforms is managed privately, which can generate a crisis. The European system, instead of delegating this decision to the Judiciary, forced the

platforms the development of a simple procedure that complains within the platform itself. This would not give more power to the platform, being different from the do-gooder technique. About regulated self-regulation, which is applied in Germany by NETZDG, he stated that it would be an interesting implementation example. Mr. Diogo Moyses Rodrigues, Coordinator of Idec's Telecommunications and Digital Rights Program, reminded of the consumerist vision regarding the topic of digital platforms regulation. He emphasized that the terms of use must be clear and accessible, and the rules for content removal must be communicated in a simple and transparent way. There should be, in these cases due process and appeal, which are within the quality of service provision. Even if notification about certain content is waived, the right to information should remain. With regard to accountability, there must be transparency about targeting and boosting, and these must be public.

In the 3rd public hearing, held on 08/12/2021, with the theme "Content Moderation and Freedom of Expression", Ms. Alana Rizzo, YouTube's Public Relations Manager, highlighted that YouTube has more than 2 billion users worldwide and that the content reflects the reality of real-life discussions. That the platform has rules and that they remove 10 million videos per quarter. He then addressed the platforms' policies for removing content that violates community rules. He indicated that there are 3 notices for removal and a link to challenge the platform's decision, which creates a reduction of questionable content. He said that YouTube rewards creators of content within the rules and that inappropriate videos represent only 0.18% of the platform's total content. He stressed the importance of freedom of expression and the platform's right to correct errors in moderating its content. Next, Mr. Jonas Valente, Associate Professor at Lapcom, UnB's Communication Policy Lab, pointed out that generic content moderation rules have not been enough. And that one should work with a public and democratic regulation. But we also shouldn't allow abuse by public authorities. He defended that PL 2630 should have the capacity to update the norms and, therefore, the establishment of a supervisory authority seems interesting. As for moderation procedures, there should be a guarantee of user notification, and Codes of Conduct should list the content that can be removed immediately, without a contradictory. Mr. Márcio Novaes, President of Abratel, the Brazilian Association of Radio and Television, highlighted the freedom of the press and the prohibition of anonymity. People's freedom of expression does not prevent the responsibility of the press vehicles, or the intermediaries. He sustained that the difficulty of separating what is internet and what is platform makes it difficult to build specific rules for the latter. In this sense, platforms should assume responsibilities similar to those incident on traditional media. Regulatory asymmetry between the two should be ended. Next, Tai Nalon, Executive Director of Aos Fatos, highlighted the role of fact-checkers and defended the responsibility of authorities according to their influence in the information scenario. She stressed that disinformation should be focused on the coordinated behavior of users and not the media, and that transparent data access policies should also be encouraged. Then, Mr. Paulo José Lara, Coordinator of Article 19's Digital Rights Program, said that the internet should not be reduced to platforms or social networks, and that the PL should be drafted to increase access to information and encourage public debate. Priority should be given to freedom of expression and human rights, and not only to transparency. The participation of civil society and platform users, he said, is essential, in addition to the State and the platforms themselves. He argued that companies cannot use their economic power to increase political power. Mr. Marcelo Träsel, President of the Brazilian Association of Investigative Journalism Abraji, said that we already have several mechanisms that can be applied in cases of abuse regarding disinformation. The journalistic practice must be protected, avoiding the removal of journalistic content just for disagreeing with its content. He informed that there are a large number of requests for removal of content by politicians, and ruled out the need for the creation of a criminal type of disinformation, but that it would be problematic to do so, either because academically it is not well defined, or because many of them are directed against news companies. Finally, Mr. Diogo Coutinho, Professor of

Economic Law from USP and representative of ABIPAG - Brazilian Association of Payment Institutions said that retailers are increasingly dependent on online payment platforms. In other words, retailers depend on the Big Techs, which have high market power in their performance niches, being true *gatekeeprs of* the internet. Thus, non-discriminatory access to these platforms should be guaranteed and content moderation should not lead to discriminatory practices for people who depend on these payment methods.

In the 4th public hearing, held on 08/17/2021, with the theme "Paid Content, Advertising and Boosting on Social Networks", we highlight the speech by Mr. Marcelo Bechara, that one should differentiate advertising from boosting. In this sense, freedom of expression would be different from the right to "viralize" user content. Mr. Francisco Cruz said that different advertisements need to be treated differently. Political or electoral advertising should receive more attention, because it is more sensitive. And there should also be different treatment when there are public resources involved in the advertising. Mr. Alexandre Gibotti argued that, as a rule, every time boosted content is published the platforms should be jointly responsible for the content.

In the 5th public hearing, held on 08/19, with the theme "Protecting Democracy from Disinformation: a Shared Responsibility", Mr. Diogo Rais talked about hypotheses of shared responsibility among several actors. Then, Ms. Monica Steffen said that fact-checkers are important and Facebook works today with more than 80 fact-checkers, reducing the reach of news considered false in the feed. Following, Mario Leite argued that the civil police is in precarious conditions to fight online crimes. Mr. Marcelo Rech, in turn, defended the valorization of the journalism profession, which serves as a counterpoint to the dissemination of fake news by Big Techs. Then, Mr. Luiz Augusto makes a defense of the use of fact-checkers in content moderation by digital platforms. Finally, Mr. Paulo Renáinformed that anonymity is important for whistleblowers and disinformation is done by messages from known people. He added that traceability solutions are of great concern, because keeping records of the chain of referrals breaks end-to-end encryption, among other problems.

In the 6th public hearing, held on 08/24/2021, on the theme "How to Identify Malicious Agents without Harming Data Protection?", Mr. Danilo Doneda, Professor at IDP, Public Law Institute, defended that there are problems in relation to traceability with personal data protection, because it is massified and incompatible with the idea of minimizing risks and contrary to *privacy by design*. Even the restricted use for groups is not pertinent, and there is impropriety in foreign solutions that have not even been implemented properly. The best would be systems with metadata analysis and user reports. Next, Ms. Jaqueline Abreu, researcher and member of the PDP Jurists Commission - Personal Data Protection, defended that the Brazilian Legislation already foresees several types of ways to fight illicit acts, such as interception, search and seizure, etc. The problem would be the lack of resources and training, which gives the impression of lack of surveillance tools. He said that traceability goes against the protection of personal data. It is necessary to focus on who is in daylight, with identifiable profiles, making fake news. Director Miriam Wimmer, from the National Data Protection Authority, pointed out that there is a preponderance of freedom of expression and that the LGPD is not an anti-fake news norm, but concerns the way data travels on the network. And the problem is the targeting and granularity of other forms of communication. In this context, care should be taken not to treat data excessively, as this can pose other risks. Finally, he defended that it is precious to be cautious about identification and tracking rules, taking into account the principle of necessity. Ms. Bruna Martins Dos Santos, representing Data Privacy Brasil, stated that the fight against misinformation should go hand in hand with personal data protection policies. She also stated that the ANPD has a central role in the discussion of possible measures to combat disinformation. According to her, the wording of the current art. 7 leaves users vulnerable to eventual leaks of personal data, especially of identity documents. She added that the traceability instruments proposed in the

PL are ineffective, besides putting encryption at risk. Samara Castro, INPD member, stated that one of the most current and challenging debates is how to identify and punish perpetrators of crimes in the digital environment without hurting the principles of privacy and data protection. She reinforced that it is fundamental to define criteria between what is interpersonal communication and what is mass communication. An interesting criterion, according to her, would be the "gateway" to participation in each virtual communicational environment. Finally, Mr. João Brant, Director of the Culture and Democracy Institute, said that disinformation is a violation of freedom of expression and access to reliable, plural and diverse information. He also argued that disinformation is a major contemporary problem in Brazil, which has negative repercussions on several democratic indicators. He added that it is a mistake to apply the dictates of privacy and data protection to a part of messaging services that should not be considered private messages, but rather social communication, with messages intended for a wide audience. For him, there should be a separation between interpersonal communication features and viral or mass communication, including by law.

At the 7th public hearing, held on 08/26/2021, with the theme "How to Combat Disinformation in Private Messenger Services", Mr. Rony Vainzof, Secretary of CONIB argued that, when the platforms reach a great political and economic power, we must demand from them some behaviors. Hate speech must be restrained, moderation criteria must be improved, and the free manifestation of thought must be weighed in order not to be extrapolated. The issue of log storage is important and should be preserved in the text of the proposal. As for private messaging services, one should differentiate between interpersonal and personal communication. Next, Mr. Diego Canabarro, Member of ISOC - Internet Society for Latin America and the Caribbean, pointed out that there are obsolescence risks of legislating focusing only on the type of service. He explained that cryptography is multidimensional, including its importance for authentication of people and machines and for ensuring privacy and the viability of criminal investigations. He warned that the traceability of Art. 10 should be rejected, as there is a breach of encryption. Then, Mr. Pablo Ortellado, professor at USP, made a counterpoint, defending that messaging services have interpersonal communication formats, but can also be used for mass communication in a deleterious way. The opacity in the routing would encourage illicit acts, and investigations lack the technical capacity to find the origin of the illicit message. He argued that Art. 10 does not break encryption because the forwarding is already stored on the server and the system operator already saves the message. Thus, he could store the message without decrypting the message. Mrs. Veridiana Alimonti, Public Policy Analyst for Latin America at EFF - Electronic Frontier Foundation, said that the proposals of art. 10 create hypothesis of previous and massive data storage and are worrying in relation to human rights and that the metadata can be used to obtain information about people. Art. 10 intends to reverse privacy protections in order to create a new layer that has a direct connection of the metadata with the content of the communication. Then, Mr. Claudio Henrique Ribeiro Da Silva, law professor at the Federal University of Ouro Preto, pointed out that the moderation of platforms is often arbitrary, with abusive application of the terms of use. A law that creates obligations for this moderation and identification of users is dangerous. Article 12 is important to establish the moderation rules, but it may serve as a varnish, a legitimacy, for the abusive moderation of content on platforms. Next, Mr. Dario Durigan, Whatsapp's Director of Public Policy, said that the company has already adopted successful measures to curb abuses of freedom of expression, such as reducing forwarding chains. In 2020, for example, it was forbidden the mass shooting of messages, an obligation followed by the company. This work, according to him, has been achieved without traceability. Art. 10 would end up identifying all mass forwarding messages from users, violating the protection of personal data and users' rights. Finally, Mr. Ivar Hartmann, a professor at INSPER, argued that Art. 10 is not about traceability of any messages. And that there are several requirements for traceability to be identified. It would only be a tiny fraction of the messages that would be tracked and the data that are recorded are the ones that indicate which users

carried out mass forwarding of the message, with date and time of forwarding and the total number of users who received the message. In addition, the data could only be used as evidence in criminal investigations and in criminal proceedings, by means of a court order. Finally, he emphasized that there would be no breach of encryption if art. 10 was adopted.

At the 8th public hearing, held on 08/31/2021, with the theme "Technology and National Sovereignty", Laura Schertel Mendes, professor at UnB and IDP, defended that freedom of expression protects not only individuals, but also the digitalized public sphere, the collectivity. This public sphere must be functional and healthy, with access for all, valuing quality information and the protection of personal data. The assumption of sovereign regulation is that it can be enforced in its jurisdiction, but this does not seem to be the main guideline, since many authoritarian states use this argument to practice censorship on the Internet. About the traceability of communication, in art. 10, there is a disproportionality between what it is intended to fight, disinformation, and the volume of information that is collected, causing a violation of privacy. Next, Mrs. Luiza Brandão, Director of IRIS, spoke, defending that we must escape from the idea of closed sovereignty, used by totalitarian states. For her, sovereignty is a two-way street that requires mutual recognition among the various countries. Art. 32 determines that ISPs must have headquarters and appoint legal representatives in Brazil. The headquarters in Brazil would not be necessary, and could harm the country. Requiring representatives may also compromise innovation and attract new companies to bring their business to the country. Next, Mr. Rodrigo Fragola, President of Assespro/DF, took the floor and argued for self-regulation as the basic principle of the PL and that there should be a more precise definition of what fake news is. Limiting by law what the platforms can moderate is dangerous, because it ties up the possibilities of self-regulation, including the technology used. Article 10 promotes mass surveillance and threatens freedom of expression, and should be deleted. Then, the Attorney Fernanda Teixeira Souza Domingos said that the problem is not the fact that the account is inauthentic, but its illicit use. For her, art.12, which deals with moderation, should be more explicit, placing more precise guidelines for the moderation activity of the platforms. Child pornography issues are generally not referred en masse and seem not to be attacked by the proposal. As for art. 26, the prosecutor said that the Council for Transparency and Accountability on the Internet should be contemplated with a representative from the Public Ministry, one from the Judiciary and one from the OAB. Finally, the obligation of installing the headquarters of the application provider in Brazil would not be necessary, he said, but the obligation of appointing a legal representative would. Mr. Ângelo José Mont Alverne Duarte, from the Brazilian Central Bank, talked more about aspects of the digitalization of the financial market, and defended that the law should be drafted in order to stimulate the entry of new competitors in the market. Finally, attorney Patrícia Peck Pinheiro said that digital relations have a transnational nature and the question is how to carry out legitimate surveillance, without jeopardizing civil rights and fundamental rights. For her, responsibility must be shared when what we have are people who are simultaneously contributing to the existence of the internet. In art. 32, the best would be to place the need for representatives and not to oblige them to have a headquarters in the country.

In the 9th public hearing, held on September 2nd, with the theme "Raising Awareness on Disinformation: the Role of Education", Mrs. Patrícia Blanco, Executive President of the Open Word Institute, said that disinformation is a complex issue, which has moved from the analog to the digital environment and has 3 fundamental axes: (i) raising awareness of the population, showing risks and damages of disinformation;
(ii) punishment for those who maliciously disseminate misinformation; (iii) more power to the citizen to criticize each information they receive. In the sequence, Caio Machado, Executive Director of Vero Institute, affirmed that research is essential for us to understand the problem and provide solutions for society, and that we must demand transparency from the platforms and demand media education and digital skills. He noted that art. 21 of the PL should introduce this need in the curricular base, education being a way to modulate behaviors. In other words, he argued that moderation should

have an educational factor. Ms. Natália Leal, CEO of Lupa News Agency, pointed out that Lupa agency has today more than 20 collaborators and it is an independent agency. As for art. 21, it should contemplate obligations on media education. The fact-checkers, in his view, increase the cost of lying in any environment, and the checking activity doesn't need its own regulation or new rules, because it is already journalism. The legal framework would already contemplate the main criminal offenses in disinformation. Next, Ms. Angela Pimenta, Director of Operations at PROJOR, spoke about the types of disinformation in digital media, highlighting the false context of some news and the *deep fake*. She explained the three phases of disinformation, which begin with creation, go through reproduction, and end with distribution. He rejected a new typification in the fight against misinformation, because journalism itself may end up losing, and noted that crimes against honor and the provision of civil damages would be enough. In his opinion, the focus should be on the method of distribution of digital content, with the promotion of factually verified content. Mr. Sérgio Lüdtke, Editor-in-Chief of the Comprova Project, explained how Comprova works, which works collaboratively with original sources, and how it differs from ordinary fact-checkers. He defended that the checking work is journalism and that they don't check journalistic vehicles, but sites that pretend to be journalistic, using software monitoring to identify news with a large volume of circulation. Professor Sérgio Amadeu Da Silveira, from UFABC - Federal University of ABC, talked about the fundamental elements of disinformation. He affirmed that distributed communication has inverted the flow in relation to mass communication, showing that today it is easier to speak and harder to be heard, and that disinformation is not based on disinformation, but on spectacularization. Criminalization, for him, is not the way out. Regarding art. 10, he defended that it generates a *looping* guard of information, generating exacerbated surveillance, and that mass shooting tools of the platform itself should be banned, with greater transparency in the performance of algorithms. Finally, Mr. João Feres Júnior, Coordinator of LEMEP - Laboratory for Media and Public Sphere Studies at UERJ, pointed out that disinformation in Brazil predates social networks, with the mainstream media as the protagonist. That newspapers often publish only the negative part of certain situations, and that education is important, but regulation is fundamental. He said that private journalism companies have very little transparency in how they generate the news, and fact-checking agencies usually do not check the mainstream media.

In the 10th public hearing, held on 09/09/2021, with the theme "Platform Diversity and Asymmetric Regulation", Ms. Natália Neris, representative of Twitter, shared the vision of an open, global and unique internet and that Twitter defends this model. The platform's service is to serve the public conversation. She highlighted important internet principles: (i) be global; (ii) have trust is essential; (iii) there must be choice and control over the rating recommendation algorithm; (iv) moderation is more than just leave or remove, it must give clear guidelines. He added that Brazil should maintain and strengthen the principles of the Marco Civil da Internet. Then, Mr. Marcel Leonardi, representative of FGV, pointed out that monopolies can be apparent and come to an end quickly with technological advancement, so one cannot focus on a snapshot of reality. He said that the regulation of the big ones can annul the emergence of small companies and that a debate about local regulation versus global internet is necessary. There is a risk, according to Marcel, of regulating local players, leaving out the small ones and also leaving out companies that don't have legal representation from Brazil. Mr. Felipe Carmona Cantera, National Secretary of Copyright and Intellectual Property, emphasized the importance of the Marco Civil da Internet for the freedom of expression and the difficulty of precisely identifying fake news. He affirmed that it is difficult to name a champion of truth. About Provisional Measure n. 1.068/2021, he pointed out that it prohibits the spreading of false news or crimes. He affirmed that social networks do not give any justification or right of defense for removing or blocking their users' content. Finally, Mr. Sérgio Branco, Representative of the Coalition for Rights on the Net, spoke, defending that there is no right to publish, because there is no corresponding duty not to publish. He explained that copyrights can be patrimonial, with economic value, and moral rights, of a personal, non-economic nature. Therefore, there would be, in principle, no copyright infringement if the work is excluded from a

certain Internet platform.

In the 11th public hearing, held on 09/14/2021, with the theme of "Good practices in combating disinformation during the Covid-19 Pandemic", Mr. João Guilherme Bastos Dos Santos, Representative of the National Institute of Science and Technology in Digital Democracy, raised 3 points: (i) social networks make up a viral information system, with each platform acting in a different way. Each worrying theme can be in different platforms; (ii) the pandemic decentralizes the information, because it generates an immediate and individual gain and it decentralizes the actors because it ends up decentralizing the income sources; and (iii) the fake news debate should go hand in hand with the data protection debate, because it is what potentializes and directs the spreading of fake news. Next spoke Mr. João Henrique Rafael Junior, creator of UPV - União Pró-Vacina, stating that the confidence of Brazilians in vaccines was already falling since 2015. During Covid, the intention to get vaccinated dropped at the end of 2020 with the advance of misinformation, but rose again in 2021. He reported that surveys indicate that the reasons for the loss of trust were related to conspiracy theories and fake news, and that platforms are indispensable with alerts about false content. Next, Mr. Thiago Tavares, president of SaferNet Brazil, sustained that it is necessary to differentiate disinformation from merely bad, or low-level information, and discussed the dynamics and steps of false advertising. It is important to note that there are also disinformation campaigns that come from outside Brazil, which can pose threats to national sovereignty. He said that the monetary issue is quite relevant, because it generates distorted incentives, and platforms should remove the possibility of *cash-out* on criminal sites or sites that convey disinformation. Mr. Mathieu Turgeon, a professor in the Department of Political Science at Western University, said that the risk factor of fake news is the alteration of cognitive disposition and the confirmation of biases and political views, and that the repetition of information makes human beings tend to believe it, creating an illusion of truth. What can we do? According to the professor, platform and media verification mechanisms, digital literacy, remove robots and automated accounts. One should not prohibit fake news or conspiracy theories by law, because they are open concepts that can inspire distrust in state action. Ms. Estela Aranha, member of the Brazilian Institute of Criminal Sciences - IBCCrim, said there is no silver bullet for Fake News and that more moderation by the platforms is needed, not less moderation, as proposed by PM 1.068/2021. He said that the art. 10 is directed to only one service and the keeping of records puts at risk the protection of data and the confidentiality of communications. It is a lot of risk and a lot of burden for a measure that is ineffective. He said it is important to create the concrete possibility of identifying the logical port of Fake News propagators, which often does not occur with the Marco Civil da Internet.

In the 12th public hearing, held on 09/16/2021, with the theme of "Impacts of a law against disinformation on the innovation ecosystem", Mr. Diego Dorgam, professor of Software Engineering at UnB, said that private messaging services and social networks are increasingly similar and it is almost impossible to differentiate how people access content on both. Thus, care should be taken not to criminalize the technology, but the people who eventually produce illicit content. Thus, care should be taken because digital identity today is associated with a cell phone number that does not guarantee true identity. Next, Mr. Marcelo Lacerda, from the Brazilian Chamber of Digital Economy - camara-e.net, talked about the digitalization of the labor market, with technology generating economic growth and opportunities for people and companies. He defended the adoption of *smart regulation*, which brings cooperation between the public and private sectors and takes into account the constant evolution of technology, always inserted in a context in flux. He opined that the differences between platforms should be taken into consideration, with technological neutrality. He noted that there are non-regulatory approaches, including through media education, that should be considered, as well as codes of conduct. Mr. Fabro Steibel, from the Institute of Technology and Society of Rio de Janeiro - ITS-Rio, said that the ideal would be to change the Marco Civil of the internet and not create new specialized legislation, and that fake news has been politicized because of the elections, but it is an old problem. The remedy for this problem, he said, seems to turn to messaging services, and what is at stake is moderation

of content and the form of the bill is very much linked to the way the big platforms work. The problem is that the proposal assumes the use of personal data and puts encryption at risk, which can generate mass surveillance. Ms. Tatiana Ribeiro, Executive Director of the Competitive Brazil Movement - MBC, stated that there are unwanted risks with the PL, which can impact the internet ecosystem in Brazil and reminded that the Economic Freedom law can avoid some regulatory abuses. He noted that it would be appropriate to have regulatory impact analyses and transaction costs to take into account costs and benefits of imposing a regulation in the suggested manner. Finally, Mr. Wanderley Mariz, Kwai's Public Policy Director, highlighted 3 important elements: compatibility and synergy with the LGPD, flexibility in foreseeing the rules, and the adoption of self-regulation mechanisms, demanding clear rules from state agents. Then, Mr. Maurício Moura, founder of IDEIA Big Data, said that surveys show that Brazilians do not trust traditional journalistic content and most have already admitted to sharing fake news. It would be necessary to make the LGPD actually adopted and implemented during the electoral elections. He informed that Canada has created legislation focused on the transparency of the electoral process and said that the responsibility should fall on the authors and not platforms, although the action of blocking the content should occur quickly. He defended that monitoring individuals is not the good way out, as it creates a dangerous precedent, and that the ideal is to identify who finances this news system. Mr. Robson Lima, president of the Brazilian Association of Telecommunications Operators and Internet Providers, sustained that the problem is not the Internet or technology, but society. In some cases, he defended, it is necessary to identify IP numbers to identify crimes, such as school killings, pedophilia and kidnappings, and therefore, it is necessary to remove and block contents quickly in more serious cases, before a tragedy occurs. Finally, Mr. Leandro Alvarenga Miranda, legal director of the National Association of Information Bureaus said that the PL transfers the responsibility from the Public Sector to private entities, in the sense that these companies should self-regulate. This would generate a risk of punishing the companies, while the ideal is to punish the wrongdoers. Disinformation must be combated, but not at the cost of those who create jobs. Regarding unauthenticated accounts, he believes that a restriction could be created on the rights of users who wish to use pseudonyms, for example. Art. 10, in his consideration, may conflict with the LGPD by suggesting the identification and tracking of users.

In the 13th public hearing, held on September 21st, with the theme "Criminalization of Disinformation - A good solution?", Mr. Marlon Reis, representative of the Movement Against Electoral Corruption, defended that the solution in the criminal scope is not efficient in all cases and that the ideal would be the criminal typification only for more extreme conducts, in the case of criminal organizations that mobilize financially in an illicit way for electoral influence and in a massive way. Outside the criminal scope, the PL could have quicker mechanisms, in the civil and electoral field, to prevent false news from spreading easily. In the electoral field, we could have some sanction of ineligibility, with its own procedure and with special representation. Mr. Fernando Neisser, from the Brazilian Academy of Electoral and Political Rights - Abradep, said that the disinformation machines are based on a tripod: first the lying ideas, then the platforms that are the access ways to the user and, finally, there are also intermediaries that provide informal databases and mask the origins of the remittances that make the investigative work more difficult. Fake news only gains penal importance when it has repercussions in society. It wouldn't make sense, according to the speaker, to control by the content, but by the structures set up to disseminate false news. He reminded that the recently changed art. 870 of the Electoral Code is a good example of a criminal type that can be effective, and that the tracking of art. 10 is quite worrying for privacy. Mr. Carlos Oliveira, from UnB, said that people use the same mechanisms to process true and false information and these mechanisms are based on previous influence, and there are psychological elements that establish biases in the reception of information, and partisanship exerts a strong conditioning. The question is whether the solutions put forward can correct this. He suggested that the attempt of correction often produces more confirmation of the bias and that the best would be to have

greater circulation of correct information. Cassiana Saad De Carvalho, head of the Division of Repression of Cyber Crimes of the Federal Police, said that criminal law cannot be trivialized, as it is the last *resort*. There is a great technical complexity in dealing with electronic evidence and the investigation tools for punishment must dialogue with reality, otherwise we will not be able to obtain the necessary evidence. In relation to penal execution, he defended that alternatives for freedom-restricting sentences must be thought of. Then, Mr. Valdemar Latance Neto, Federal Police Delegate, said that criminalizing conducts without the means to punish can generate a certain frustration. He sustained that the police must have the adequate means and there must be capacity building, training, equipment; integration among the police; cooperation between Brazil and other countries, because the suspects use transnational tools, in clouds, often using machines that are outside the Brazilian territory. Finally, there must be the collaboration of private companies with the police, to obtain the suspect's user data. Mr. Alexandre De Andrade Silva, Deputy of the Federal Police's Office of Repression of Electoral Crimes, understands that disinformation has become part of the security agenda of countries, but that criminal law should be reserved for criminal organizations and those with great social impact. Penalties in the field of ineligibility may be a good solution, but one should not only look at the content of the posts in order to seek punishment. He recalled that the art. 326-A of the electoral legislation already criminalizes the conduct of spreading false news about someone who is known to be innocent. Finally, Mr. André De Faria Pereira Neto - Researcher at FioCruz/ENSP, stated that there are solutions other than criminalizing fake news. First, fact-checking, then digital literacy, and finally information quality assessment. The more good-level information available, the better it is for fighting disinformation. He found that even websites of public entities have a low rate of compliance with correct information on the subject of public health and that there could be a kind of certification of these pages, in order to ensure that fake news are effectively combated with quality public information.

In the 14th public hearing, held on 09/23/2021, with the theme of "Changes in the Marco Civil da Internet and Accountability of Platforms", Ms. Marília Monteiro, representative of TikTok, presented the platform and its operation, and highlighted that content that violates community rules is moderated and removed. She said that the company releases transparency reports and that about 82% of videos were removed before they were published on the platform, with 150 million videos prevented from being created by automated means. The platform gives the right of appeal for content removal by reviewing the video and making the decision. There are plans to create a Center for Transparency and Accountability in the United States. In Brazil, the company has partnered with the newspaper O Estado de São Paulo and other media outlets to verify content. Next, Ms. Paloma Rocillo, representative of the Institute for Reference in Technology and Society - IRIS, said that there is global pressure to increase the responsibility of the role of intermediaries, both because of abuses and the centrality and power of platforms. In his view, the connection provider should not be held liable for third-party content, and the application provider can only be held liable if it fails to comply with a court order to remove content, but that this cannot be a blank slate. He explained that in the U.S., the good Samaritan rule exempts the application provider for the error in moderation, but that in Brazil this is not so. Although the platforms are not responsible for the initial content, other rules of Brazilian law apply to the moderation activity. The solution would be to increase the transparency of moderation activities. Mr. Raul Echeberria, representative of the Latin American Internet Association, spoke about the Brazilian laws that deal with the Internet. If approved as it is, he said there are risks of regression with PL 2630/2020 in relation to the Marco Civil da Internet, and that there must be a balance between economic development and fighting disinformation. In the legislative process, one should not find the means to predetermined ends and solutions. With PL 2630, the tendency would be a greater volume of removals, threatening freedom of expression. He pointed out that a free enterprise environment is not contrary to fighting disinformation, and that greater transparency is needed in moderation mechanisms. Mr. Emerson Wendt, Civil Police delegate, stated that cyberdamage should be avoided before publication. He addressed

the various laws that have tried to reduce cyber data in Brazil. He said that platforms are quick to meet their own terms of use, but not so quick to comply with legal rules and that the suspension of content should be done in a precautionary way if there is false news proven by message. Mr. Emmanuel Publio Dias, professor at the Escola Superior de Propaganda e Marketing - ESPM, sustained that the objectives and fundamentals of PL 2630 are very important, that the Internet is a public space that transforms communication, which used to be one-way, into something multiple-way, with broad participation. He said that automated and boosted accounts, with potential illicit use, should be regulated. He considered that advertising is the buying of the audience, and that boosted content should therefore be seen as advertisers. The problem is advertisers and content boosters that are outside of Brazil, and it is necessary to identify the payment of any kind of boost to follow the money trail. Ms. Bruna Martins Dos Santos, German Chancellor Fellow at the Alexander von Humboldt Foundation, said that the Marco Civil is the only fair and democratic instrument to mediate the relationship between users and internet application providers, since it prevents prior censorship and allows subsidiary responsibility of the platforms. He sustained that we cannot speak in immunity of platforms, but in a protection, at least partial, for the responsibility of third-party content. He pondered that censorship practiced by private actors affects freedom of expression. The attempt of PL 3227/2021 to try to say when moderation can occur, however, is not the way. The way is, in his opinion, transparency and strengthening of due process in the moderation activity. Renata Mielli, representative of the Coalition for Rights on the Net, said there are two extremes: notification and immediate removal, and the clamping down of moderation activity, making it conditional on the need for a prior judicial order. He noted that the Marco Civil did not focus on moderating content on the Internet, but the complexity of the phenomena that are occurring, and it is necessary to create more rules and obligations so that the platforms can perform the task of moderation in a more transparent and predictable way. There should be a user's right to appeal inadequate moderation, as platforms do not apply their moderation rules uniformly for everyone. He noted that moderation can be asymmetric even when the platform stops moderating and that transparency and due process (including about the team performing the moderation) are quite important changes. Mr. Marco Antonio Da Costa Sabino, representing IBMEC, said that the Marco Civil da Internet has won system the *judicial notice and take down*. It is not possible for intermediaries to be held responsible for something over which they have no control. In this sense, there is no need to change the Marco Civil, which already creates disincentives for illicit postings. If there is an eventual joint and several liability of the user with the application provider, there will be a right of recourse of the providers over the users, inhibiting freedom of expression and, at the same time, a greater incentive for the platforms to already remove, *ab initio, the* content suspected of illegality. Finally, Francisco Brito Cruz, Director of InternetLab, pointed out that the Marco Civil resolved many important conflicts, but did not intend to solve everything. There is no need to reform the Marco Civil, but a complementation, which will reach some actors. The Marco Civil's incentive system does not allow platforms to remove users' posts for fear of liability, which is good. But the Marco Civil's article 19 does not close the debate, as, for example, in the case of damage generated by the platform's own act, with an undue removal. The Executive's PL no. 3.227/2021, has good and bad parts, but the restriction on content moderation and the supervision by the Executive may violate freedom of expression.

At the 15th public hearing, held on September 28th, with the theme "Implementation and enforcement of the law: who regulates?", Mr. Demi Getschko, CEO of the Information and Coordination Center of Ponto br, stated that one of the important points of the MCI is art. 19. He emphasized that the CGI has a public note recognizing the importance of art. 19 for the preservation of freedom of expression. He defended the maintenance of the current wording of art. 19 and remembered that since the beginning of the internet there were tensions and discussions, with contents that were frowned upon by users. He also mentioned that, in 1996, there was a problem in the USA with the publication of the "decency act", which was very badly received by the internet community. Regarding the bill, he stated that there must be a definition about

what is pure distribution and a publishing activity that engages with the content. Another point is to establish the existing rules in terms of use, similar to "rules established by clubs or associations", preserving the rights established by the Constitution and the legislation in force. In short, it would be necessary to establish a taxonomy to apply rules similar to those in section 230 of the section. He also stated that it is best to evaluate what is harmful or not to the community, not what is true or false. The decisions, in the end, need a technical sieve, someone who has enough technical knowledge to evaluate the impacts of possible interventions in the Internet environment. Next, Professor Marcos Dantas Loureiro, from the Federal University of Rio de Janeiro's School of Communication and member of the Internet Steering Committee, spoke. He presented definitions about the three layers of the Internet: application, Internet infrastructure and telecommunications infrastructure, stating that, recently, there has been a growing debate about how to regulate the layer of "content" offered through applications. He pointed out that the CGI.br has very similar attributions to those foreseen for the Transparency and Accountability Council foreseen in the proposition. Thus, according to him, the CGI.br could assume such attributions foreseen in the PL, taking advantage of the expertise already developed by the CGI.br in regulating and supervising the functioning of the Internet in Brazil. Mrs. Bia Barbosa, representative of the Coalizão Direitos na Rede, understands that a fundamental element for the discussion about eventual new internet rules is the definition of the actors responsible for the implementation and supervision of the current rules. For her, the existence of a multi-sectorial organ for inspection and production of studies about the theme is essential. She also emphasized that the regulation of the network must include dynamic arrangements capable of adapting to the rapid changes in the network. According to her, the CGI.br would be the ideal place to carry out such attributions, as it already has almost 3 decades of history in multisectoral performance in internet governance. Next, Mr. Marcelo De Souza Do Nascimento, General Director of PROCON/DF, spoke about the connection between the dissemination of false information and consumer rights. According to him, one deals daily with misleading advertisements on the internet that have a structure very similar to that of fake news. He pointed out that in the PL, in the form approved in the Senate, there is express mention to the maintenance of the guarantees and principles of the Consumer Defense Code. He also mentioned that several internet applications, such as social networks, have become important channels for the commercialization of goods and services. He also stated that, even with the enactment of the LGPD, there is still an intense circulation of consumers' personal data on the Internet, which directly harms consumers' rights. Regarding enforcement, he pointed out that not even the Procons have an arm to oversee the dissemination of false news related to the consumer market. Mr. Pedro Vaca, OAS Special Rapporteur for Freedom of Expression, warned that the technical complexity and importance of the Internet requires that any change in the rules of its use should occur only after broad public discussion, and that there are several attempts to capture the public debate in the world by entities and individuals who invest in the dissemination of misinformation. For him, there are three frontiers that should not be crossed, paths that are not recommended: regulatory excesses, exclusivity of rules in self-regulation; and intuitive and accelerated solutions. He argued that internet regulations should be routinely reviewed and modernized, preferably in a way that dialogues with national paradigms and international practices, under a paradigm harmonious with international internet governance. For this reason, multilateralism would be an interesting possibility, which can build standards and help propose solutions in a democratic way and debated in depth by experts. Finally, Mr. André Iizuka, representing the Brazilian Association of Electronic Commerce - ABCOMM, presented the structure of the Brazilian Association of Electronic Commerce, founded in 2014, with

9,000 member companies. According to him, it is the only legitimate representative of the segment.

On 11/9/2021, a Working Group meeting was held with representatives from academia, the business sector, and academia. At the meeting 25 participants gave their contributions. Mr. Thiago Tavares, from Safernet, conceptualized moderation and stated that the new law should be something that helps give effectiveness to the Marco Civil da Internet and the LGPD, including through tools such as a *call center*. The focus of regulation should start with

outsourcing activities. Mr. Francisco Brito Cruz from Internetlab highlighted important points in the text, such as the fact that platform decisions are made on a large scale and should therefore be constantly monitored, and that requirements such as Portuguese language teams in moderation and specific reports for Brazil, rather than global, are necessary. Mr. Fabro Steibel from ITS defended the exclusion of remuneration for journalism companies from the text and said that it could be clearer that part of the proposal applies to some and part applies to all. He questioned whether a model of regulated self-regulation is really effective, or whether the State should put its weight behind it. Ms. Kalianna Puppi defended the possibility of lawful discrimination by platforms. That it is imperative to distinguish between what is lawful and what is not. She also pointed out that some transparency suggestions are unfeasible, such as, for example, providing the number of Brazilian users who use the platform. He also suggested that there should be the possibility of no appeals when the case involves the publication of very serious content, such as pedophilia. Ms. Karen, from Youtube proposed reformulating the definition of instant messaging services to clearly exclude e-mails, as the Federal Senate's wording did. Ms. Flávia Xavier Anneberg of Google said that several articles do not apply to search engines, since they do not constitute a social network, have no followers, etc. She opined that the remuneration of journalistic companies ends up discouraging the search for information. Mr. Igor Ferreira, from Camara-net, proposed the exclusion of search engines, the sanctions of suspension and exclusion, and the requirement of representation in Brazil, which can result in market concentrations. Mr. Felipe França raised several points that deserve revision, highlighting the problem of automated accounts, the risk of imposing exaggerated sanctions that could harm the consumer, and the exclusion of the criminal type, since the country already enjoys several legislations that could solve the problem being sought. Ms. Renata Miele highlighted the importance of the transparency report, arguing that it does not contain unreasonable demands. She affirmed that the CGI will perform better than the Transparency Council proposed by the Federal Senate. He said he was in favor of the exclusion of art. 36, which deals with the issue of remuneration of journalism companies. Ms. Caroline from ABIPAG showed concern for small and medium retailers, so that there may be a healthy competition environment without discrimination in the many different markets that make up the Internet. Mr. Diogo Coutinho, from USP, stated that the PL is about more than fake news. That the internet is a large infrastructure, more than just a network that conducts content. In this sense, he argues that it is necessary to create a scenario in which small and medium-sized companies are not discriminated in their business models, so that they can compete with the platforms. He said it is necessary to raise the minimum number of users for the application of the law, to about 21 million registered users. Ms. Ana Paula, from Brasscom, warned that excessive transparency rules can be used by bad actors to circumvent usage rules, including trade secrets. As for automated account highlighted that it is not always bad and that profiling should not be linked to LGPD. Mr. Samir Nobre, from Abratel, expressed support to the substitute and said that the remuneration to journalistic companies is welcome. He suggested that art. 36 be complemented by the legislative proposal in this sense presented by Deputy Filipe Barros. Ms. Lailla Malaquias, from Twitter, expressed concern that the legislation may become obsolete quickly. She pointed out that the use of automated accounts can be positive, as they provide many useful services to users. It would be ideal to put a mechanism to prohibit only the illicit use of automated accounts. Adriele Britto, from Assespro, pointed out problems with the sanctions of art. 29, especially those of suspension and prohibition. She suggested that it could be reduced to 0.5%. Raquel Cândido, from Aba, pointed out that the freedom of the actors must prevail and that there are already mechanisms that guarantee, in an efficient way, the self-regulation of advertising in Brazil. Mr. Diego de Lima Guald, from IAB, pointed out that one should be aware of the negative consequences not intended by the text. He pointed out that there is already a concept of advertising in the legislation, which can generate confusion with the already existing concept of propaganda. He proposed that arts. 19, 20 and 21 be reconsidered. Marcelo Bechara, representative of the Freedom with Responsibility Coalition, affirmed that disinformation has been a cancer in Brazilian society. He pointed out that the Brazilian advertising law is not respected and that internet platforms only started to act against disinformation recently, with the pandemic. Ivar Hartmann, from

Insper, said that there was progress in the changes in the Substitutive and that the library of ads should be broad enough, not containing only electoral propaganda. The reports, in his opinion, should maintain ample transparency. He pointed out that the European legislation brings many requirements that are scattered and not in the same device, with which the transparency criteria in Brazil are compared. Therefore, he explained, there would be no greater requirements in the Brazilian proposal. Mrs. Bia Barbosa, from CGI.br, emphasized that the attributions given by the proposal to the managing committee are not foreign to CGI's current activities. She emphasized that, however, there are concerns from committee members about the new attributions. Mr. Dario Durigan, from WhatsApp, pointed out that there were advances, but that the art. 12, I, still represents a very broad intervention in the company's business model, establishing a fence that would make the service worse for the user. He also pointed out that users could end up using chips from other countries to cheat the system, which would make the solution empty. Mr. Juliano Maranhão - Legal Grounds Institute, congratulated the rapporteur's work and emphasized that the transparency mechanisms must cover all aspects of technical management of possible abuses. Not only of the moderation result, but of its process. For him, there should be easier access for scientific institutions with well-delimited projects to the platforms' data, so that the former can effectively contribute to the debate. Mr. João Paulo Bachur, from IDP/CEDIS highlighted that the chapter on public agents and art. 13 are meritorious and brought advances, and that the moderation of the platforms is an important activity to stimulate the freedom of expression and not to restrict it. He noted that the institution of rules for the remuneration of journalism by application providers may result, in practice, in reduced access to news. Mr. Diogo Rais, from the Digital Freedom Institute, warned not to confuse content that merely quotes a congressman with content that broadcasts electoral propaganda. According to him, search engines would be in a complicated situation to differentiate, identify and moderate the amount of content with quotes to candidates and differentiate it from electoral propaganda. Finally, Mr. Jonas Valente, from the Public Policy Lab of UnB, understands that the insertion of search engines in the text of the proposal was not artificial and that there are several activities of these platforms that deserve regulation. He also pointed out that the current reports do not give the information in a sufficiently transparent way.

To the main proposition were joined Bills No. 1676/2015, authored by Congressman Veneziano Vital do Rêgo, 2712/2015, authored by Congressman Jefferson Campos, 6812/2017, authored by Congressman Luiz Carlos Hauly, 7604/2017, authored by Congressman Luiz Carlos Hauly, 8592/2017, authored by Representative Jorge Côrte Real, 9533/2018, authored by Representative Francisco Floriano, 9554/2018, authored by Representative Pompeo de Mattos, 9647/2018, authored by Representative Heuler Cruvinel, 9761/2018, authored by Representative Celso Russomanno, 9838/2018, authored by Representative Arthur Oliveira Maia, 9884/2018, authored by Representative Fábio Trad, 9931/2018, authored by Representative Erika Kokay, 10860/2018, authored by Representative Augusto Carvalho, 200/2019, authored by Representative Roberto de Lucena, 241/2019, authored by Representative Junior Ferrari, 346/2019, authored by Representative Danilo Cabral, 1974/2019, authored by Representative Reginaldo Lopes, 2601/2019, authored by Representative Luis Miranda, 2602/2019, authored by Representative Luis Miranda, 3389/2019, authored by Representative Fábio Faria, 3857/2019, authored by Representative Jaqueline Cassol, 4925/2019, authored by Representative Moses Rodrigues, 5260/2019, authored by Representative Nereu Crispim, 5776/2019, authored by Representative Afonso Motta, 5959/2019, authored by Representative Luizão Goulart, 6351/2019, authored by Representative Luis Miranda, 283/2020, authored by Representative Cássio Andrade, 437/2020, on behalf of Alexandre Frota, 475/2020, on behalf of Capitão Alberto Neto, 517/2020, on behalf of José Medeiros, 693/2020, on behalf of Alexandre Padilha, 705/2020, on behalf of Célio Studart, 808/2020, by congressman José Guimarães, 988/2020, by congressman Alexandre Frota, 1258/2020, by congressman Luis Miranda, 1394/2020, by congressman Zé Vitor, 1941/2020, by congressman Wilson Santiago, 2196/2020, by congressman Alexandre Frota, 2284/2020, by Alexandre Frota, 2389/2020, by Rejane Dias, 2763/2020, by Marcelo Brum, 2790/2020, by José Nelto, 2844/2020, by Joseildo Ramos, 2854/2020, by

Deputy Maria do Rosário, 2883/2020, authored by Deputy Filipe Barros, 3029/2020, authored by Deputy Alexandre Frota, 3044/2020, authored by Deputy Paulo Ramos, 3063/2020, authored by Deputy Felipe Rigoni, 3119/2020, authored by Deputy Mário Negromonte Jr, 3144/2020, by Joice Hasselmann, 3222/2020, by Frei Anastacio Ribeiro, 3307/2020, by Alexandre Frota, 3395/2020, by Bia Kicis, 3573/2020, by Luiz Philippe de Orleans e Bragança, 3627/2020, by Nereu Crispim, 4418/2020, by David Soares, 127/2021, by Nelson Barbudo, 213/2021, by Luiz Philippe de Orleans e Bragança, 246/2021, by Caroline de Toni, 291/2021, by Daniel Silveira, 356/2021, by General Girão, 388/2021, by Carlos Jordy, 449/2021, by Igor Kannário, 495/2021, by Dra. Soraya Manato, 649/2021, by Pedro Lucas Fernandes, 865/2021, by Ronaldo Carletto, 1001/2021, by Helder Salomão, 1362/2021, by Daniel Silveira, 1589/2021, by Dra. Soraya Manato, 1590/2021, authored by Deputy Renata Abreu, 1743/2021, authored by Deputy Giovani Cherini, 1772/2021, authored by Deputy Luiz Philippe de Orleans e Bragança, 1897/2021, authored by Deputy Alexandre Frota, 1923/2021, authored by Deputy Alexandre Frota, 2060/2021, by congressman Altineu Côrtes, 2390/2021, by congressman Emanuel Pinheiro Neto, 2393/2021, by congresswoman Renata Abreu, 2401/2021, by congressman Reinhold Stephanes Junior, 2831/2021, by congressman Capitão Alberto Neto, 2989/2021, by congressman Marx Beltrão, 3366/2021, by congresswoman Rejane Dias, 3700/2021, by congressman José Guimarães, 4134/2021, by congressman Carlos Bezerra, 143/2022, by congressman Coronel Armando, 714/2022, by Congressman Nereu Crispim, 836/2022, by Congressman Eduardo Bolsonaro, 2516/2022, by Congressman José Nelto, 125/2023, by Congresswoman Sâmia Bomfim, 1087/2023, by Congressman Guilherme Boulos, 1116/2023, by Congressman Hercílio Coelho Diniz.

In short, Bills #3063/2020, 3627/2020, 3389/2019, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6351/2019, 3044/2020, 1591/2021 and 2763/2020 address the prohibition of the use of automated accounts on internet platforms.

Bills #3063/2020, 3144/2020, 2883/2020, 127/2021, 1362/2021 and 865/2021 bring obligations to use fact-checkers to analyze misinformation on internet platforms.

In turn, Bills #3063/2020, 283/2020, 2854/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 3385/2020, 291/2021, 449/2021, 3573/2021, 213/2021, 495/2021, 2401/2021, 127/2021, 246/2021, 1362/2021, 865/2021, 2390/2021, 649/2021, 10860/2018, 5776/2019, 475/2020, 4418/2020, 4925/2019, 5260/2019, 865/2021, 1087/2023, 1116/2023, 2516/2022, 836/2022, 2712/2015, 437/2020, 2284/2020, 6531/2019, 7604/2017, 9647/2018, 346/2019, 517/2020, 1116/2023, 1087/2023, 3395/2020, 2601/2019, 2602/2019, 1941/2020, 2196/2020, 2831/2021, 3700/2021, 1589/2021, 1897/2021, 5959/2019, 143/2022, 1772/2021 and 2060/2021 establish rules and criteria for the removal or restrictions on content, which may imply curtailment of the right to freedom of expression and on the providers' responsibilities.

The Bill 3144/2020 creates the requirement for a regulatory body for issues related to disinformation on the Internet. Bill No. 1974/2021 creates the National Week to Combat Fake News and creates the National Day to Combat Fake News to be celebrated every April 1st of each year.

Bills #s 3063/2020, 3144/2020, 283/2020, 3029/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 449/2021, 127/2021, 1362/2021, 2390/2021, 1743/2021, 2989/2021, 3366/2021 e 1590/2021 establish various transparency parameters to be met by Internet platforms with regard to misinformation.

Bills #1676/2015, 8592/2017, 9554/2018, 9554/2018, 9533/2018, 9761/2018, 9838/2018, 9884/2018, 9931/2018, 200/2019, 241/2019, 3307/2020, 693/2020, 705/2020, 1394/2020, 988/2020, 6812/2017, 1923/2021, 1258/2020, 1941/2020, 2389/2020, 2790/2020, 1001/2021,

2196/2020, 3857/2019, 4134/2021, 2844/2020, 3222/2020, 356/2021 e 388/2021 create criminal types or penalties for various conducts that disseminate false information.

The proposition and the attached were distributed, initially, to the Committees of Science and Technology, Communication and Information Technology and of Finance and Taxation, for consideration on the merits, under art. 54, of the Internal Rules of the House of Representatives - RICD, and for the Committee of Constitution and Justice and Citizenship for analysis on the merits. The proposal is subject to the Plenary's appreciation and the processing regime is that of priority, pursuant to art. 151, II, of the RICD.

On June 21, 2021, a Presidential Act published in the House of Representatives Gazette, Supplement, Pages 5-6, on June 23, 2021, created the Working Group to analyze and prepare an opinion on Bill No. 2630 of 2020, and related bills, which aims to improve the Brazilian legislation on Internet freedom, responsibility, and transparency.

In all, the Working Group held, in person and remotely, 27 technical and deliberative meetings, including 15 public hearings, with the participation of more than 150 specialists on the subject, who had the opportunity for a wide and fruitful debate on the topic.

On 11/28/2021, we presented a first formal report proposal (REL 1/2021 GTNET) and, on 01/22/2021, after deliberations and technical meetings with the deputies, a new report was presented (REL 2/2021 GTNET). Then, on 12/1/2021, we presented a complementary vote, based on suggestions made by the members of the working group. Finally, on 12/1 and 12/07/2021, respectively, after several deliberative meetings, the basic text of the proposal was approved and the suggestions presented by the deputies were voted on, consolidating the text that we will present below.

The matter was sent to the Committees of Labor, Administration, and Public Service; of Social Security and Family; of Science and Technology, Communication, and Informatics; to the Committee of Finance and Taxation, for analysis of the merit and verification of financial and budgetary adequacy; and to the Committee of Constitution and Justice and Citizenship, for analysis of the merit and examination of constitutionality, legality, and legislative technique.

Due to the distribution to more than three merit commissions, it was then determined that a Special Commission be created to analyze the matter, as provided for in item II, of article 34, of the Internal Rules of the House of Representatives (RICD).

A request for urgency was approved, and the matter is now ready for consideration in Plenary.

This is the report.

II – RAPPORTEUR'S VOTE

I consider this project meritorious and timely, considering that the emergence of the Internet has revolutionized the ways of communication, allowing information to be accessed directly by people, potentially transforming each user of the world wide web into a source of content. The Internet's end-to-end model allows the flow of data and content to circulate more freely, fostering the rights of freedom of expression and increasing access to information.

Internet freedom, although enabling the network society and realizing several fundamental rights, brings with it some negative externalities. One of them is the false news or, as they have been commonly called, the *fake news*. Ubiquitous information has generated a scarcity of audience, and it is increasingly necessary that the content somehow manages to capture the public's attention. In this sense, fake news, clickbaits, are instruments increasingly used.

The emergence of an ecosystem conducive to the propagation of

disinformation creates competing versions of the truth and accuracy of news, which makes it extremely difficult to differentiate between verified facts and pure disinformation. An MIT study, for example, found that the top 1% of fake news stories can reach up to 100,000 people on average, while true news stories rarely reach more than a thousand people.

The effects of misinformation can be fatal for democracy, since it reduces the cognitive capacity of the population, influences the electoral process, damages competing political views and silences dissenting voices, impoverishing the debate and the multiplicity of world views. The most varied experiences, ranging from the lynching of reputations on social networks, through the intimidation of journalists and public figures, to the professional production of distorted news for political and economic purposes, show the gravity of the problem and the need to confront it.

Several countries, such as Germany and France, have already imposed obligations on digital media in order to regulate the dissemination of misinformation, including deadlines and actions. In Germany, a law was passed in 2017 that deals with the removal of content from the internet. The law applies to social networks with more than 2 million users, which does not include journalistic content companies. Under this law, content related to specific articles of the Criminal Code is considered illegal, including threats to democracy, rule of law, national defense, and public order - threats, incitement of the masses, descriptions of violence -, religious, ideological, or sexual self-determination offenses; dissemination or production of child pornography; and insult, defamation, and falsification of evidentiary materials.

According to this legislation, social networks that receive more than 100 complaints annually must publish a report describing the procedures used, authors of complaints by category of users, experts and associations consulted, blockages made and reaction times (24h, 48h, etc). In procedural terms, social networks must acknowledge complaints immediately and remove or block access to manifestly illegal content within 24 hours of receiving the complaint, within 7 days for non-manifest complaints, and within longer periods if clarification is requested from the user or if the content in question is derived to an independent verification entity. The verification institutions must be paid for by the social networks and the penalties, applied by the Ministry of Justice, can reach up to 500,000 euros in case of refusal to provide information and up to 5 million euros in other cases.

France, meanwhile, issued its legislation, "Fight against Information Manipulation," in 2018. First, it amended the Electoral Code to determine that, during the three months preceding and until the date of the electoral vote, relevant digital services must: (a) indicate the contractors of sponsored content when related to debates of general interest; inform how personal data will be used in content related to debates of general interest; and publish aggregate information; (b) when there are inaccurate or misleading allegations or accusations of a fact that could affect the fairness of the elections and are deliberately, artificially or automated and massively disseminated by electronic means, the judge may, at the request of the public prosecutor, any candidate, any party or group or interested person, act to prevent such dissemination within 48h.

In addition, the French law amended the Freedom of Communications Act (Law 86-1067) to allow the Higher Audiovisual Council to reject a broadcaster's work plan (mandatory for television channels) that contains broadcasts that pose a serious risk of attacking human dignity, freedom and property, plurality of thought and opinion, protection of children and adolescents, public order, national defense, or the fundamental interests of the Nation, including the regular functioning of its institutions.

During the three months preceding the election, if false information is deliberately disseminated that could alter the impartiality of the election, the Council can order the suspension of the transmission of the electronic communication service until the conclusion of the election, subject to an appeal within 48 hours.

At the Internet level, French law has established that online service providers must: i) include a device indicating that the content is false, especially when sponsored; ii) identify the

contractors of sponsored content in debates of general interest; iii) to carry out educational actions; iv) to inform the Council about the measures taken; v) to appoint an interlocutor and legal representative for this purpose.

It is worth noting that part of the French law was declared partially unconstitutional, but relevant parts, including the one described in the last paragraph, survive.

More recently, two important pieces of legislation were passed, the Digital Services Act - DSA and the Digital Markets Act - DMA. In the Digital Markets Act, Internet intermediation platforms must comply with a series of obligations since they are "fundamental structuring elements of the current digital economy, responsible for the intermediation of most transactions between end users and professional users".

As far as we are concerned, the Digital Services Act came into force on 11/22/2022, effective as of 02/17/2024. The regulation governs the obligations of digital services that act as intermediaries, connecting consumers with goods, services, and content. The overall goal is to protect users and their fundamental rights online by establishing uniform transparency and *accountability* mechanisms across Europe.

The DSA fights illegal online content (arts. 4, 9 of the DSA) by adopting mechanisms that allow users to identify and *flag* illegal online content. Such illegal content is defined as "any information which, by itself or in connection with an activity, including the sale of goods or the provision of services, does not comply with Union law or the law of any Member State, whatever the subject matter or precise nature of that law. There is also an obligation of own initiative on the part of providers or intermediaries (arts. 7 and 8 of the DSA), encouraging providers to conduct, in good faith and diligently, voluntary own-initiative investigations to identify, remove or block access to illegal content. Such action does not eliminate the eventual hypothesis of non-accountability of platforms in relation to third-party content.

Another point of the DSA is the action against illegal content (art. 9 of the DSA). The competent judicial or administrative authorities may issue a decision against certain unlawful content and the platforms must act against such content and inform of the follow-up that was given to the situation, specifying if and when the order was executed. Such decision should be quite detailed, including: (i) the legal basis of the order; (ii) information identifying the issuing authority; (iii) information enabling the platform to identify the specific recipient or recipients in respect of whom information is sought, such as account names or unique identifiers; (iv) a statement of reasons; (v) information on the redress mechanisms available to the platform.

Also according to the DSA (arts. 11 and 12), intermediary service providers must designate a single point of contact that allows them to communicate directly, electronically, with the authorities. Platform users are also entitled to a point of contact with the platforms. On legal representation, Article 13 of the DSA states that intermediaries who do not have an establishment in the European Union but offer services in the Union must designate in writing a natural or legal person to act as their legal representative. Such representative must have the necessary powers and sufficient resources to ensure efficient and timely cooperation with the authorities.

Another important issue is the obligation to submit transparency reports (art. 15 of the DSA). In this sense, information must be presented annually about any content moderation activity, including the categorization of the moderation, whether on its own initiative or due to illegal content or a request from the competent authority, among other hypotheses. The following must also be informed

use of automated means for content moderation purposes, including a qualitative description, the objectives, accuracy indicators and possible error rate of such automated means.

An Internal Complaints Management system was also instituted (art. 20 of the DSA), in which platforms must maintain, for a minimum period of six months after a moderation decision, access to an effective internal complaints management system that allows users to submit complaints, electronically and free of charge, against the decision taken by the platform. This applies to decisions that: a) delete information, block access or restrict its visibility; b) suspend or terminate the provision of the service, in whole or in part, to recipients; c) suspend or terminate recipients' accounts; d) suspend, terminate or otherwise restrict the ability to monetize information provided by recipients.

Furthermore, under art. 22 of the DSA, the state may certify certain companies as *fact checkers for the* purpose of notifying the platform to remove illegal content. A trusted fact checker must: (i) possess specialized knowledge and specific skills for the purpose of detecting, identifying and notifying illegal content; (b) be independent of any platforms; (c) conduct its activities with a view to submitting notifications in a diligent, accurate and objective manner. Signaling companies must publish an annual transparency report and their actions must be monitored to avoid excesses.

Boundaries and measures have been established and protection against abusive use (art. 23 of the DSA). Here, platforms may suspend, for a reasonable period of time, people and accounts that act abusively both in publishing illegal content and in reporting and unfounded complaints about illegal content from third parties. Such procedures should be done transparently and be very clear in the platforms' terms and conditions of use.

Another interesting approach is the explicit prohibition of the so-called *dark pattern* (art. 25 of the DSA). Providers of online platforms may not act with the aim of misleading or manipulating the recipients of their service or to distort or substantially impair the ability of users to make free and informed decisions about the content to be accessed. This includes, for example, giving more prominence to certain options than others when asking the user of the service for a decision, or making the procedure for cancelling a service more difficult than subscribing to it.

Regarding the rules for advertising (art. 26 of the DSA), users of the service must be able to identify clearly, concisely, unambiguously and in real time: a) what content constitutes an advertisement, through clearly visible signage; b) the beneficiary of the advertisement, i.e. the person on whose behalf the advertisement is displayed; c) the person paying for the advertisement, if different from the beneficiary; d) relevant information, directly and easily accessible from the advertisement, about the main parameters used to determine the recipient of the display of the advertisement and, if applicable, how to change these parameters.

The DSA has established obligations regarding the transparency of the recommendation algorithm (art. 27 of the DSA). In this case, platforms must be transparent, in their terms of use, in clear and simple language, about what are the main parameters used in their recommendation systems, as well as any options that allow recipients of the service to change or influence these parameters. The user must be informed about the most significant criteria for determining the information suggested to him and the reasons for the relative importance of these parameters.

Risk assessment obligations (arts. 33 to 36 of the DSA) have also been adopted on the part of large platforms. It is worth noting that the DSA considered that large platforms are those with more than 45 million users within the European Union, must identify, analyze and diligently assess all systemic risks potentially arising from their services, including algorithmic systems. As for systemic risks, these include the spread of illegal content, negative effects

actual or foreseeable in the exercise of fundamental rights, in civic discourse and electoral processes, and in public safety, and also potential negative effects in relation to violence against women, the protection of public health, and minors, and serious negative consequences for a person's physical and mental well-being.

Thus, upon detection of specific risks, platforms should adopt reasonable, proportionate and effective mitigation measures tailored to the situation-specific systemic risks. Such measures may include: (a) adapting their content moderation processes, including the speed and quality of handling notifications for specific types of illegal content; (b) testing and adapting their algorithmic systems, including their recommendation systems; (c) using or adjusting the cooperation with trusted beacons; (d) adopting specific measures to protect children's rights, including age verification and parental control tools.

In case of serious threats, the authority may require platforms to identify and implement specific, effective and proportionate measures to prevent, eliminate or limit the said serious threat. For this, there is a very detailed procedure.

Another relevant point of the European norm concerns the independent audits (art. 37 of the DSA), to which the large platforms must submit, at least once a year, and which will be paid for by the platforms themselves, aiming to verify compliance with the measures imposed by law.

On recommender systems (art. 38 of the DSA), large platforms using them must offer at least one option for each of their recommender systems that is not based on profiling. In other words, an obligation to have alternative algorithms. There are also Obligations to provide access to data (art. 40 of the DSA) necessary to monitor and evaluate compliance with this regulation.

In addition, a supervisory fee was instituted (art. 43 of the DSA) for supervisory activities of the authorities in relation to compliance with the obligations set out in the law. The amount of the fees will be determined by the European Commission and will vary depending on the type of platform and the activities to be supervised, and must follow certain criteria, such as the actual costs of supervision and an overall limit of 0.05% of the platform's annual worldwide net income in the preceding fiscal year.

A relevant issue concerns Codes of Conduct (Arts. 45-47 of the DSA), the development of which by platforms will be encouraged by the EU to address challenges arising from illegal content and systemic risks. In the latter case, authorities may invite platforms and civil society to participate in the development of codes of conduct setting out commitments to take specific risk mitigation measures. The Commission and the national authority can assess whether the Codes of Conduct meet the specified objectives. In case of persistent non-compliance, the Commission and the authorities can invite the signatories of the codes to take the necessary measures.

European legislation has also determined that member states must designate one or more competent authorities as responsible for the supervision of intermediary service providers and for the enforcement of this Regulation (articles 49 to 51 of the DSA). The authority must be "fully independent", remain "free from any direct or indirect external influence and may neither seek nor take instructions from any other public authority or from any private entity". The European Commission retains powers to oversee large platforms.

Quanto às sanções, previstas no art. 52 do DSA, estas serão definidas pelo Estados-membros separadamente, mas devem atender aos seguintes parâmetros: (i) em caso de descumprimento de uma obrigação prevista no DAS, a multa deve ser de, no máximo, 6% do volume de negócios anual a nível mundial da plataforma no exercício anterior; (ii) caso haja fornecimento de informações incorretas, incompletas ou enganosas, ausência de resposta ou não retificação de informações incorretas, incompletas ou

misleading or the refusal to submit to an inspection, the fine must be a maximum of 1% of the platform's annual worldwide income or turnover; and (c) the maximum amount of the fines must correspond to 5% of the average daily worldwide turnover or average daily income of the platform in the previous financial year, calculated from the date specified in the decision in question. It is worth noting that users (art. 54 of the DSA) of the platforms' service have the right to claim compensation from the platforms in respect of any loss or damage suffered due to the breach of the obligations under the DSA.

In the United States, both the previous president and the president have asked for changes in the text of the so-called section 230, of the Communications Decency Act. The rule was created in the 1990s for two purposes. First, to exempt application providers from liability for third-party content, and second, to allow them to remove obscene, sensual, or lewd content, for example. Successive extensive interpretations by the courts of the provision turned Section 230 into a kind of right to moderate third-party content on the part of application providers, who came to enjoy editorial rights without the corresponding duties on the part of traditional media.

Furthermore, in the United States there are important discussions in the judiciary, such as the case of Nextchoice v. Paxton, which discusses the limits of the right to free speech in the moderation activities of large platforms.

In light of this, it is urgent that we can rebalance the digital environment, especially in social networks and private messaging services, so that they can be instruments that foster freedom of expression and civilized and factual discussion of our people's political differences.

It is, therefore, with great satisfaction that we report the Bill of Law No. 2.630, of 2020, which establishes the Brazilian Law of Freedom, Responsibility and Transparency on the Internet. It is a comprehensive and bold proposal, which aims to create an environment that, while minimally regulated, preserving the fundamental freedoms of expression and access to information, establishes the possibility of controls over false news.

In chapter I, the proposal sets out the preliminary provisions, which include the scope of the law, the principles and objectives to be adopted, and the definitions to be used when applying this proposal.

Along the lines of our Substitutive Bill, we decided to extend the application of the law to application providers that are search engines, in addition to social network providers and private messaging services, which we now call instant messaging. The application of this legislative proposal applies only to providers that offer services to the Brazilian public and exercise activity in an organized manner, whose number of registered users in the country exceeds 10,000,000 (ten million).

In addition, we also cover application providers offering on-demand content, regardless of the number of users, for copyright issues.

Providers whose activities are performed by a legal entity based abroad are also under the aegis of the proposal. In any case, providers that are non-profit online encyclopedias, scientific and educational repositories, open source software development and sharing platforms, closed platforms for virtual meetings by video or voice, scientific and educational repositories, tools for searching and making available data obtained from public authorities, especially from the bodies and entities provided for in Article 1 of Law No. 12,527 of November 18, 2011, and online gaming and betting platforms are excluded.

Furthermore, we determine that the legal entities referred to in the caput of art. 2 will be considered media for the purposes of art. 22 of Complementary Law 64, of May 18, 1990, in order to

that it is possible to ascertain misuse, misappropriation, or abuse of economic power or authority, or misuse of providers, to the benefit of a candidate or political party.

We have incorporated to the list of principles the protection of public health, a topic of unquestionable relevance in itself, but that, in the midst of the Covid-19 pandemic, has gained even more prominence. We have added the duty to prohibit the unlawful or abusive discrimination of users by the services of the providers referred to in the proposal, including as to updated data and the non-restriction of technical functionalities, except in cases of non-compliance with the provisions of this proposal.

Moreover, we have added the principles contained in several laws, such as those included in Law No. 4,680 of June 18, 1965 - Legal Framework for Advertising Activities, Law No. 12,529 of November 30, 2011, which structures the Brazilian Competition Defense System, Law No. 13,709 of August 14, 2018 - General Law of Personal Data Protection, and Law No. 14,197 of September 1, 2021, which typifies crimes against the Democratic State of Law. We also added a paragraph stating that freedom of expression is a fundamental right of the users of the providers mentioned in this proposal, under the terms of art. 5, item IX, of the Federal Constitution.

In regards to the objectives, in art. 4, we highlight desiderata such as the strengthening of the democratic process and the promotion of the diversity of information in Brazil, the guarantee of transparency of the providers in relation to their activities with the user, including on their procedures for elaborating and modifying their terms of use, the adoption of moderation and recommendation criteria for content, and the identification of advertising or promoted content.

Thus, we lend greater importance to ensuring transparency, the adversarial process, the full defense and due process in relation to procedures for the application of terms of use and other policies of the platform, in particular when it comes to measures that restrict freedom of expression or the functionality of content and accounts of its users, including cases of exclusion, unavailability, reduction of scope or flagging of content and accounts. We have added the goal of ensuring transparency about procedures for drafting terms of use policies and other policies of our own. We have added to the objectives of the initial proposal the limitation of the use of data of any nature, including personal data, and the principle of free enterprise, as a limiting element on the impetus of the regulatory force incident on the services provided by the providers.

In art. 5, we chose to exclude the definition of identified account, since the purpose of the text is to focus efforts on tackling disinformation, rather than to propose any broad and general identification regime for internet users in Brazil. We also excluded the definition of inauthentic account, which may lead to restrictions on the constitutional use of pseudonyms and users' freedom of expression.

We altered the definition of social networks, with the wording adopted in part in PL no. 3227/2021, which we believe is more precise and in line with the present proposal. We chose to remove the final part of the definition, which refers to the legal entity that performs activities for economic purposes and in an organized manner, by offering services to the Brazilian public, so that the definition does not conflict with the provisions of art. 2, which deals with the scope of the law, and that mentions providers whose activities are performed by legal entities based abroad.

We also changed the wording of the definition of an automated account to one that is managed wholly or predominantly by a computer program or technology to simulate, substitute, or facilitate human activities and that is not provided by the provider itself. A

The new definition is clearer and avoids ambiguous expressions, which could create doubts.

We define instant messaging services as internet applications whose primary purpose is to send instant messages to certain specified recipients, including the offer or sale of products or services and those protected by end-to-end encryption, other than electronic mail services. We exclude e-mail services.

Next, we define a search engine as an internet application that allows the search by keywords of content prepared by third parties and available on the internet, grouping, organizing and ordering the results according to relevance criteria chosen by the platform, regardless of the creation of accounts, user profiles or any other individual registration, including content indexing. We exclude from this definition those search tools that are intended exclusively for e-commerce functionalities.

Similarly, we have included the definition of profiling, as being any form of data processing, automated or otherwise, to evaluate personal aspects of a natural person, with the aim of classifying them into groups or profiles, or for behavioral profiling or personal profiling referred to in the LGPD.

In Chapter II, Section I, we define the civil liabilities, which are incumbent upon ISPs in each situation. In this sense, the providers will be jointly and severally civilly liable: (i) for the repair of damages caused by contents generated by third parties whose distribution has been carried out through platform advertising; and (ii) for damages arising from contents generated by third parties when there is a breach of duty of care obligations, in the duration of the security protocol dealt with in Section IV.

In Section II, we discussed the obligations to analyze and mitigate systemic risks. In such cases, providers must diligently identify, analyze, and assess systemic risks arising from the design or operation of their services and their related systems, including algorithmic systems. That assessment shall involve the design and operation of their services and their related systems, including algorithmic systems.

The risks to be addressed are those related to the dissemination of illicit content within the scope of the services according to the caput of art. 11, and the damage to the collective dimension of fundamental rights in the cases determined by law, such as the right to freedom of expression, information and the press, and the pluralism of the media or civic, political-institutional and electoral issues.

In performing the risk assessment, providers will take into consideration factors such as the design of their recommendation systems and any other relevant algorithmic systems, their content moderation systems, their terms of use and their enforcement and the influence of malicious and intentional manipulation on the service, for example. In view of the presence of these factors, providers will adopt reasonable, proportional and effective mitigation measures directed at systemic risks by adapting their services, their terms of use, as well as the criteria and methods of their application, among other obligations.

It is worth noting that when automated tools are used, there must be human supervision and verification to ensure accuracy, proportionality and non-discrimination. To ensure the monitoring of the providers' actions, they must grant within a reasonable period of time, in the form of regulation and upon request and whenever requested, access to data that contribute to the detection, identification and understanding of systemic risks.

Next, in Section III, we detail the obligations of the so-called duty of care, in which the providers must act diligently to prevent or mitigate illicit practices within the scope of their service. This action includes concentrating efforts to improve the combat against some illegal contents generated by third parties, among them crimes, such as those against the Democratic State of Law and coup d'état, acts of terrorism, crime of inducement, those of instigation or aid to suicide, crimes against children and adolescents provided for in Law No. 8069 of July 13, 1990, and discrimination or prejudice.

Regarding the duty of care, we will evaluate, among other materials, the information provided by the providers in the systemic risk and transparency evaluation reports, and the treatment given to the receipt of notifications and complaints. To avoid a possible sanction on the lack of duty of care of individual contents or a small set of them, we determine that the evaluation will always be performed on the set of efforts and measures adopted by the providers.

We then deal, in Section IV, with the obligations in situations of imminent risk of harm, which will run that occur: (i) when imminent risk of harm to the collective dimension of fundamental rights is configured; in the foreseen cases of duty of care; or (ii) in the breach of obligations established in the systemic risk assessment section.

In such cases, a security protocol can be established for a period of up to 30 days, a procedure of an administrative nature whose stages and objectives must be the subject of its own regulation. The goal is to create a mechanism to supervise the providers.

Providers may, as of the establishment of the security protocol, be held civilly liable for damages arising from content generated by third parties when prior knowledge of such content is demonstrated and the measures provided for in this proposal have not been adopted. Such liability will be joint and several when there is imminent risk of damage during the duration of the protocol and will be restricted to the subjects and hypotheses stipulated therein.

We chose to suppress the content of art. 7 of the text approved by the Senate, as we understand that it results in the formation of unnecessary registries and increased data collection by the applications, in violation of the necessity principle, provided by the General Law of Data Protection - LGPD. Furthermore, ISPs are not, nor should they be, experts in processing and identifying the veracity of user identifying information. This minimizes the possibility of the formation of an organized mass identification registry, reducing the discretionary power of social network providers and private messaging services to obtain personal data contained in identities and the consequent burden on users' privacy.

In the sequence, we deliberated for the complete exclusion of art. 8, also from the Federal Senate. First, because the rule creates one more barrier to internet access and communication for an economically vulnerable group, increasing the digital exclusion. Second, because the communication between the telephone companies and the messaging applications about the numbers that had contracts cancelled by the operators implies the development of detailed database interconnection procedures, with harmful consequences to privacy, security, territoriality of the applications and costs, which must be taken into consideration. Moreover, the obligations tend not to solve the problem, since the use of numbers from abroad, or the temporary use of "leased" numbers, can easily circumvent the measure.

In Chapter IIII we address moderation procedures, refining and including several rights and safeguards for ISP users. This item was the subject of much discussion in the public hearings and several of the appendices to this legislative proposal.

We have established guidelines for the application of the moderation rules of the providers that may lead to exclusion, unavailability, reduction of scope or flagging of content generated by third parties and their accounts, as provided in the terms of use and policies. In such cases, the providers must notify the user of the nature of the measure applied and its territorial scope, its rationale, pointing out the clause applied or the legal basis for its application, what are the procedures and deadlines for the right to review the decision, and whether the decision was made exclusively through automated systems.

To facilitate contact with the user, we propose that the platforms make available their own channel, highlighted and easily accessible, for a minimum of six months, to consult the information provided, in order to facilitate the formulation of complaints about content and accounts and to send requests for review of decisions. Providers will be responsible for giving a reasoned and objective answer to requests for revision of decisions, as well as providing for their immediate reversal as soon as an error is verified.

We have foreseen hypotheses of publicization of content moderation actions, determining that ISPs must create mechanisms to publicly inform the moderation action and keep public the identification of the judicial action that originated the moderation in contents and accounts.

In Chapter IV, which deals with transparency in boosting and advertising issues, we have added more information to the Senate's text to be provided by ISPs. We have determined, for example, that the providers must make available in an accessible manner, with clear information, in the Portuguese language, the terms of use of their services, which must include, among other information, a concise summary with the main characteristics of the services and the main elements contained in the terms of use, the types of prohibited content, the age range for which they are intended, and the potential risks of use. In addition, we have established that providers are required to disclose in their terms of use the governance measures adopted in the development and use of automated systems to further protect users.

We also maintained the mandate to deliver biannual transparency reports, which must be made available on the providers' websites, with easy access, in Portuguese, in order to inform content moderation procedures, under the terms of the regulation.

Furthermore, we have established that ISPs must, by default, require human action and user consent for the activation of automated content playback, except for music content and playlists created by the user him/herself, and we forbid ISPs to encourage changes to this standard. In addition, we determine that ISPs must adopt technical measures that enable the identification of recommended content clearly, unequivocally and in real time, so as to differentiate it from the content selected by the user.

In Section IV of this chapter we have adopted the suggestion that providers should conduct and publish annually an external and independent audit to assess compliance with the provisions of this proposal, the codes of conduct, and the regulations, addressing a minimum list of issues, such as the efficiency in fulfilling the obligations of systemic risk analysis and mitigation, the level of efficiency, accuracy, precision, and coverage of the mitigation measures adopted, and the non-discrimination or absence of bias in their moderation decisions.

Finally, in Section V of Chapter IV, we determine the possibility of opening the providers' information to researchers who will have free access to disaggregated data, including by means of application programming interface, for academic purposes, provided, of course, that commercial and industrial secrets are observed.

In Chapter V we address the issue of digital advertising, approximating the treatment of this advertising with those of other media. We determined, for example, that the provider as well as the programmatic advertising platforms must require the identity of all advertisers of platform advertising, whether the individual or legal entity on whose behalf the advertising is presented, or the person who pays for the advertising.

The desideratum of the chapter was greater transparency. In this sense, we obliged the provider to make available mechanisms to provide users with information on the history of advertising content with which the account has had contact in the last 6 months. In addition, we demanded greater transparency for the criteria and procedures used for profiling users.

Next, in Chapter VI, we deal with copyrights and related rights. If such content is used on ISPs, including those offering on-demand content and produced in any format that includes text, video, audio or image, there must be remuneration to its holders by the ISPs.

Then, in Chapter VII, we did the same for the journalistic content used by the providers, which, regardless of the format, will entail remuneration to the journalistic companies. This counterpart will take the form of regulation, which will detail the criteria, the way to assess values, negotiation, conflict resolution, transparency, and the valorization of professional journalism at the national, regional, local, and independent levels.

In Chapter VIII, which deals with the actions of the Public Authorities, we have added a new provision to give greater protection to public interest accounts, in order to avoid intervention actions that impact the circulation, availability, promotion, reduction of the reach or removal of content from these accounts. In this case, we have provided for the express possibility of filing a suit for their restoration, in an expeditious manner, with the Judiciary Branch obliging the providers to restore these accounts when it is proven that they operate in conformity with fundamental rights and with the principles of legality, impersonality, morality, publicity, and efficiency.

If the user of an institutional account has more than one account at a provider, he/she shall indicate the one that officially represents his/her term of office or position to the respective regulating body, the others being exempt from the obligations of this article. In such cases, the regulatory body will forward the list of accounts indicated as institutional to the social network providers within a certain period. Furthermore, an account considered to be non-institutional will be considered as such if it contains predominantly official manifestations related to the position of these agents or public servants.

We also established the guarantee of the extension of material parliamentary immunity to platforms maintained by social media application providers.

As for the allocation of public resources for advertising on websites and social network accounts, we forbid this to occur when there is the promotion of violent speech aimed at committing crimes against the democratic rule of law.

In addition, we prohibit the public administration from contracting advertising with providers that are not incorporated under Brazilian law and are not represented in the country. This will avoid the influx of public resources to companies that are not subject to the Brazilian legal system.

For transparency purposes, we have included a provision that requires the Public Administration to make available and specify the information about resources invested in advertising destined to means of communication, including internet application providers, electronic sites, and accounts in social networks. Finally, we have established that any disciplinary punishment or act practiced by a hierarchical superior that causes damage to a public servant due to content shared privately by the latter, outside the exercise of his or her duties, and that does not constitute material whose publication is expressly prohibited by law, constitutes an unlawful act, punishable under criminal and administrative law.

Furthermore, we have established that the commercialization of advertising for insertion by providers domiciled abroad must be carried out and recognized by their representative in Brazil and in accordance with the legislation governing advertising in the country, when destined for the Brazilian market.

We have also determined that ISPs must make available to users, by means of easy access, the viewing of all boosted electoral advertising content.

Finally, we have extended the obligations regarding the history of the boosted content and advertising the user has had contact with in the last 6 months, to include information regarding the criteria and procedures used for profiling that were applied in each case.

In Chapter IX we deal with the promotion of education, imposing duties on the State for the provision of educational services that include training, integrated with other educational practices, for the safe, aware and responsible use of Internet applications. This includes campaigns to prevent misinformation and violent speech based on discrimination of sex, race, ethnicity, and religion, and to promote transparency about sponsored content.

An important theme we have added is that of children and adolescents in Chapter X. The goal was to make providers, in their services accessible by children, always have their best interests at heart, adopting appropriate and proportionate measures to ensure a high level of privacy, data protection and safety.

In Chapter XI, we address instant messaging service providers. Here we determine the limitation of forwarding messages or media received from another user to multiple recipients and establish that broadcast lists can only be

forwarded and received, in any event, by people who are identified, at the same time, in both the senders' and recipients' contact lists. The goal was to reduce, in some way, the circulation of potentially harmful and false news by reducing the reach and movement of such content across messaging platforms.

In a new device, we dispense with the adoption of the solution proposed by article 10 of the Senate Bill no. 2630/2020, which allows tracking and which, according to many of the voices heard in the public hearings held, has the potential to create a scenario of mass surveillance, with the storage of massive volumes of metadata. There would be the risk of cases of preventive monitoring of communications using this information, which could serve to intimidate individuals, violate the presumption of innocence and the secrecy of communications, breaking the expectation of privacy.

For purposes of combating online crime, we provide that a court order may order instant messaging services to preserve and make available sufficient information to identify the first account reported by other users when illegal content is being sent.

We also create an obligation for IM providers for commercial use to develop measures so that the service is used strictly for institutional or commercial purposes, i.e., to promote their products and services. The aim is to prevent the facilitation of large-scale automated triggering to multiple users. In these cases, the information must identify the sender of the message and it is forbidden to use this service for electoral or party propaganda purposes, or to distribute any content that is not related to institutional and commercial purposes. If the ISP identifies forwarding of messages that do not fall within the scope of the commercial service, it will block the offending account.

All these innovations aim to provide greater legal security for network users, reduce the potential impact of false news, and make it possible to identify the author of disinformation.

In Chapter XII, we define the role of the Judiciary, foreseeing that court decisions that determine the immediate removal of illicit content related to the practice of crimes foreseen in the law must be complied with by the providers within 24 hours, under penalty of a fine. In addition, when the ISP becomes aware of information that raises suspicion about a life threatening crime, it must immediately inform the competent authorities of its suspicion.

In the sanctions chapter, number XIII, we established the sanctions of (i) warning, (ii) daily fine, (iii) simple fine, of up to 10% of the economic group's revenue in Brazil in its last fiscal year, limited, in total, to R$50,000,000.00, (iv) publication of the decision by the violator; (v) prohibition to process certain databases, and (vi) temporary suspension of activities.

We emphasize that, although the imposition of suspension sanctions has been quite polemic, highlighting the famous case of Whastapp blocking, which generated great popular clamor, the measure is necessary for the proper enforcement of the law. As for the amount of the fines, we limited them to the absolute value of R$ 50 million reais, per violation, and opted to direct it to the Fund for the Defense of Diffuse Rights.

In Chapter XIV, after suggestions from dozens of attached bills, we created the crime of promoting or financing, personally or through third parties, coordinated action, through the use of automated accounts and other means or expedients not directly provided by the internet application provider, the mass dissemination of messages that contain a fact that is known to be untrue and that is capable of compromising the hygiene of the electoral process or that may cause damage to physical integrity and is subject to criminal sanction.

In our view, the criminalization of coordinated actions with the use of robots, automated accounts or other means not made available by the provider demonstrates the bad faith and the great risk of disinformation, deserving the opposition of a criminal type in the case of criminally punishable content or demonstrably untrue and criminally punishable facts that

cause harm to people's physical integrity or are capable of compromising the hygiene of the electoral process.

In Chapter XV, we assigned some competencies to the Brazilian Internet Steering Committee - CGI.br. Among these related competencies we highlight those of presenting guidelines for the elaboration of codes of conduct and of validating them, after their elaboration by the providers.

We altered the Federal Senate's text, which provides that ISPs must have their headquarters and appoint legal representatives in Brazil. We determined, on the other hand, that the providers must be represented by a legal entity in Brazil, and that this information must be easily accessible in the companies' electronic sites. In addition, the providers and their representatives will be responsible for delivering to the administrative authorities that have legal authority to request, under the terms of the legislation, registration information regarding Brazilian users. It is important that companies, even if they are technology companies, respect Brazilian laws and it is possible to locate and sanction them, if necessary. However, we see the obligation to have headquarters in the country as excessive and onerous, which may end up driving away investments and the efficient development of the market.

In addition, we determine that said provider representation must have full powers to respond in the administrative and judicial spheres, to provide the competent authorities with information relating to the operation, terms of use, and policies applicable to the expression of third parties and the marketing of the provider's products and services, to comply with judicial determinations, and to respond to any penalties, fines, and financial implications that the company may incur, especially for failure to comply with legal and judicial obligations.

It is important to note that, in relation to the Senate's text, we have excluded the change in Law 10,703, of July 18, 2003, proposed in the Federal Senate, since we believe that the requirement to appear in person to register to obtain telephone lines has the effect of creating obstacles to access to communication, increasing the digital divide.

In relation to the change promoted in the Marco Civil da Internet, we opted to exclude the definitions of Internet application access records, IP naming, and logical ports, as they are imprecise and at the same time dispensable for the purpose of the device.

Nevertheless, we opted, in this provision, to insert in the concepts of connection and application logs the so-called "logical gateway" and to insert registration data in the ISPs' safekeeping obligations. All with the objective of facilitating police and administrative investigations. As for the Marco Civil da Internet, we also added that the civil liability foreseen in this law is an exception to the provisions of Article 19 of that law.

Furthermore, due to the dynamism of technology, we have established a period of 5 years as of the publication date of this Law, for its revision, to be prepared based on the information generated by the biannual transparency reports, taking into account the procedures and decisions related to the moderation of accounts and content.

Finally, we established a *vacatio legis of*: (i) 12 months, as of the publication date, for arts. 7º to 10 and 23 to 25; (ii) 90 (ninety) days, as of the publication date, for arts. 12 to 15, 20 to 22, 26 to 30, 32, 38, 39, 40 and 45 to 47; and (iii) on the publication date, for the remaining provisions.

In general, we welcomed, directly or indirectly, proposals in the appendices that dealt with prohibiting or restricting automated accounts, imposing rules for the removal or restriction of posting or access to content, that provided for transparency requirements for ISPs, and that proposed criminal prosecution for cases of organized operations to disseminate false information.

On the other hand, we rejected legislative proposals from the appendices that brought about the obligation to adopt fact-checkers, that created a regulatory body, or that provided for criminal types whose core was mainly creating or individually forwarding content that was considered false.

II.1. Budgetary-financial adequacy

The Internal Rules of the House of Representatives (IR, arts. 32, X, "h", and 53, II) and the Internal Rules of the Finance and Tax Committee (NI/CFT) define that the examination of compatibility or adequacy will be conducted through an analysis of the conformity of the proposal with the multi-year plan, the budget guidelines law, and the annual budget. In addition, the NI/CFT prescribes that the analysis will also be guided by other rules related to public revenues and expenses. The Federal Constitution and the Fiscal Responsibility Law (Lei de Responsabilidade Fiscal - LRF) (Complementary Law No. 101, of May 4, 2000) are considered to be other norms.

Article 1, §1, of the NI/CFT defines as compatible "the proposition that does not conflict with the rules of the multi-year plan, the budget guidelines law, the annual budget law, and other legal provisions in effect" and as adequate "the proposition that adapts, adjusts, or is covered by the multi-year plan, the budget guidelines law, and the annual budget law.

In addition, article 1, §2 of the NI/CFT prescribes that proposals that involve an increase or decrease in revenues or expenses of the Federal Government or impact in any way on the respective budgets, their form or content, must be submitted to a budgetary and financial compatibility or adequacy examination. However, when the matter does not have budgetary and financial implications, article 9 of the NI/CFT determines that it must be concluded in the final vote that it is not up to the Commission to state whether the proposition is adequate or not.

That said, regarding the financial and budgetary compatibility and adequacy of the project, we see no conflicts.

II.2. Presuppositions of constitutionality

We note that there is no objection to the constitutionality of Bill 2.630, of 2020, or to the substitute proposed here.

Most of the proposals and the substitute meet the formal constitutional precepts concerning the legislative competence of the Union, the attributions of the National Congress and the legitimacy of parliamentary initiative.

Regarding the material constitutionality, there is also harmony between the proposed changes with the provisions of the Major Law.

With regard to legality, the projects and the substitute of the Economic Development, Industry, Commerce and Services Committee are adequate. The chosen means are appropriate to achieve the intended objective. The respective content is general and in harmony with the general principles of Law.

In terms of legislative technique, the proposals conform to the precepts of Complementary Law No. 95 of 1998, which provides for the preparation, amendment, and consolidation of laws.

II.3. Merit

Finally, on the merits, we understand that Bill No. 2.630/2020, in the form of the Substitute we now present, should be approved. This is a worthy proposal that will greatly contribute to the transparency and responsibility of social network providers, search engines and instant messaging services, as well as internet users. Moreover, the proposal we analyze here is essential to define, in a precise and effective way, fundamental rules and principles to regulate the platforms and establish solutions for the treatment of false news and disinformation within the World Wide Web in Brazil, safeguarding the constitutional fundamental rights and contributing to a more civilized and serene social interaction in the virtual environment.

II.4 - Conclusion of the vote

In view of the above, we vote:

(i) by the fact that the matter does not imply an increase or decrease in public revenue or expenses, and that it is not appropriate to pronounce on the budgetary and financial adequacy of Bill no. 2630/2020, and of the attached Bills nos. 3063/2020, 3627/2020, 3389/2019, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6351/2019, 3044/2020, 1591/2021, 2763/2020, 3063/2020, 283/2020, 2854/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 3385/2020, 291/2021, 449/2021, 3573/2021, 213/2021, 495/2021, 2401/2021, 127/2021, 246/2021, 1362/2021, 865/2021, 2390/2021, 10860/2018, 5776/2019, 475/2020, 4418/2020, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6531/2019, 7604/2017, 9647/2018, 2601/2019, 2602/2019, 808/2020; 1941/2020, 2196/2020, 1897/2021, 3063/2020, 3144/2020, 283/2020, 3029/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 449/2021, 127/2021, 1362/2021, 2390/2021, 1743/2021, 1590/2021, 9553/2018, PL 1676/2015, PL 1394/2020, PL 988/2020, PL 1923/2021, PL 1258/2020, PL 2389/2020, PL 2790/2020, PL 1001/2021, PL 1974/2019, PL 8592/2017, PL 9931/2018, PL 200/2019, PL 241/2019, PL 705/2020, PL 3222/2020, 9838/2018, 9884/2018, 3307/2020, 9554/2018, 346/2019, 2712/2015, 693/2020, 2831/2021, 3700/2021, 2989/2021, 4134/2021, 1897/2021, 3857/2019, 2844/2020, 356/2021, 388/2021, 5959/2019, 1772/2021, 2060/2021, 3366/2021 and 143/2022; PL 714/2022; PL 836/2022; PL 2516/2022; PL 125/2023; PL 1087/2023; PL 1116/2023, in the form of the attached Substitute;

(ii) for the constitutionality, legality and good legislative technique of Bill No. 2630/2020, and the attached Bills Nos. 3063/2020, 3627/2020, 3389/2019, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6351/2019, 3044/2020, 1591/2021, 2763/2020, 3063/2020, 283/2020, 2854/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 3385/2020, 291/2021, 449/2021, 3573/2021, 213/2021, 495/2021, 2401/2021, 127/2021, 246/2021, 1362/2021, 865/2021, 2390/2021, 10860/2018, 5776/2019, 475/2020, 4418/2020, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6531/2019, 7604/2017, 9647/2018, 2601/2019, 2602/2019, 1941/2020, 2196/2020, 1897/2021, 3063/2020, 3144/2020, 283/2020, 3029/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 449/2021, 127/2021, 1362/2021, 2390/2021, 1743/2021, 1590/2021, 9553/2018, 9838/2018, 9884/2018, 3307/2020, 9554/2018, 346/2019, 2712/2015, 693/2020, 2831/2021, 3700/2021, 2989/2021, 4134/2021, 1897/2021, 3857/2019, 2844/2020, 356/2021, 388/2021, 5959/2019, 1772/2021, 2060/2021, 3366/2021, 143/2022, PL 714/2022, PL 836/2022, PL 2516/2022, PL 125/2023, 1087/2023 and PL 1116/2023, in the form of the attached Substitute; and

(iii) on the merits, for the **APPROVAL** of Bill No. 2630/2020, and of the attached Bills Nos. 3063/2020, 3627/2020, 3389/2019, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6351/2019, 3044/2020, 1591/2021, 2763/2020, 3063/2020, 283/2020, 2854/2020, 2883/2020, 649/2021, 3119/2020, 2393/2021, 3385/2020, 291/2021, 449/2021, 3573/2021, 213/2021, 495/2021, 2401/2021, 246/2021, 2390/2021, 10860/2018, 5776/2019, 475/2020, 4418/2020, 4925/2019, 5260/2019, 437/2020, 2284/2020, 6531/2019, 7604/2017, 9647/2018, 2601/2019, 2602/2019, 1897/2021, 3063/2020, 283/2020, 3029/2020, 649/2021, 3119/2020, 2393/2021, 449/2021, 2390/2021, 1743/2021, 1590/2021, 9553/2018, PL 1589/2021, PL 3395/2020, PL 6812/2017, PL 9533/2018, PL 9761/2018, 9838/2018, 9884/2018, 3307/2020, 9554/2018, 346/2019, 2712/2015, 693/2020, 2831/2021, 3700/2021, 2989/2021, 4134/2021, 1897/2021, 3857/2019, 3366/2021, 143/2022, PL 714/2022, PL 836/2022, PL 2516/2022, PL 125/2023, PL 1087/2023 and PL 1116/2023, in the form of the attached Substitute, and for the **REJECTION** of Bills nos. 3144/2020, 127/2021, 1362/2021, 865/2021, 2844/2020, 1974/2019, 3222/2020, 356/2021, PL 517/2020, 388/2021, 5959/2019, 1772/2021, 2060/2021, 8592/2017, 9671/2018, 9931/2018, 200/2019, 241/2019, 705/2020, 1394/2020, 988/2020, 1923/2021, 1676/2015, 1258/2020, 1941/2020, 2389/2020, 2790/2020, 1001/2021 e

Hall of Sessions, on April 27, 2023

Deputy ORLANDO SILVA
Rapporteur □

SUBSTITUTIVE TO PLAN No. 2.630, of 2020

(ATTACHED BILLS N^OS PL 3063/2020, PL 3144/2020, PL 3627/2020, PL 1676/2015, PL 2712/2015, PL 346/2019, PL 283/2020, PL 2854/2020, PL 3029/2020 , PL 2883/2020, PL 649/2021, PL 3119/2020, PL 1589/2021, PL 2393/2021, PL 2831/2021, PL 3395/2020, PL 291/2021, PL 449/2021, PL 3700/2021, PL 3573/2020, PL 213/2021, PL 495/2021, PL 2401/2021, PL 127/2021, PL 246/2021, PL 1362/2021, PL 865/2021, PL 2390/2021, PL 10860/2018, PL 5776/2019, PL 475/2020, PL 4418/2020, PL 1743/2021, PL 3389/2019, PL 4925/2019, PL 5260/2019, PL 437/2020, PL 2284/2020, PL 6351/2019, PL 517/2020, PL 3044/2020, PL 1590/2021, PL 2989/2021, PL 2763/2020, PL 6812/2017, PL 7604/2017, PL 9647/2018, PL 2601/2019, PL 2602/2019, PL 8592/2017, PL 9554/2018, PL 9554/2018, PL 9533/2018, PL 9761/2018, PL 9838/2018, PL 9884/2018, PL 9931/2018, PL 4134/2021, PL 200/2019, PL 241/2019, PL 3307/2020, PL 693/2020 (9), PL 705/2020, PL 1394/2020, PL 988/2020, PL 1923/2021, PL 1258/2020, PL 1941/2020, PL 2389/2020, PL 2790/2020, PL 1001/2021, PL 2196/2020, PL 1897/2021, PL 3857/2019, PL 1974/2019, PL 2844/2020, PL 3222/2020, PL 356/2021, PL 388/2021, PL 5959/2019, PL 1772/2021, PL 2060/2021, PL 3366/2021, PL 143/2022, PL 714/2022, PL 836/2022, PL 2516/2022, PL 125/2023, PL 1087/2023, PL 1116/2023)

Establishes the Brazilian Law of Freedom, Responsibility and Transparency on the Internet.

Author: SENADO FEDERAL; Senator ALESSANDRO VIEIRA
Rapporteur: Deputy ORLANDO SILVA

The National Congress decrees:

CHAPTER I
PRELIMINARY PROVISIONS

Art. 1 The Brazilian Law of Freedom, Responsibility, and Transparency on the Internet is hereby instituted, with the purpose of establishing rules and transparency mechanisms for providers of social networks, search engines, and instant messaging, as well as guidelines for their use.

Sole paragraph. The prohibitions and conditions provided for in this Law will not imply in restrictions to the free development of the individual personality, to free expression and artistic, intellectual, satirical, religious, political, fictional, literary manifestation, or any other form of cultural manifestation, under the terms of arts. 5 and 220 of the Federal Constitution.

Art. 2º This Law applies to the following providers that, when constituted as a legal entity, offer services to the Brazilian public and exercise activities in an organized manner, and whose average number of monthly users in the country exceeds 10,000,000 (ten million):

I - social networks;

II - search tools;

III - instant messaging; and

IV - as to the provisions of art. 31, also the application providers offering on-demand content.

§ 1 This Law does not apply to providers whose primary activity is

I - of e-commerce;

II - for holding closed meetings by video or voice;

III - non-profit online encyclopedias;

IV - scientific and educational repositories;

V - open source software development and sharing platforms;

VI - search and availability of data obtained from the public power, especially from the members of the Public Power provided for in art. 1 of Law No. 12.527, of November 18, 2011; and

VII - online gaming and betting platforms.

§ For the purposes of this law, all the legal entities referred to in the caput will be considered media for the purposes of the provisions of art. 22 of Complementary Law 64, of May 18, 1990.

Art. 3 The application of this Law must observe the following principles:

I - the defense of the Democratic State of Law;

II - the strengthening of the democratic process, political pluralism, freedom of conscience, and the freedom of association for lawful purposes;

III - the free exercise of religious expression and worship, whether in person or remotely, and the full exposition of their dogmas and sacred books;

IV - freedom of expression, freedom of the press, access to information, the promotion of diversity of information in Brazil, and the prohibition of censorship in the online environment;

V - the free development of personality, dignity, honor, and image;

VI - the protection of personal data and privacy;

VII - ensuring the reliability and integrity of information systems;

VIII - the transparency and responsibility of the providers in the application of the provisions of this Law and its terms of use;

IX - the prohibition of unlawful or abusive discrimination by ISPs against users;

X - consumer protection;

XI - the protection of public health;

XII - free enterprise; and

XIII - those foreseen in the following normative diplomas:

a) Law No. 4.680, of June 18, 1965 - Legal Framework of Advertising Activity;

b) Law No. 8.078, of September 11, 1990 - Consumer Defense Code;

c) Law No. 12,965, of April 23, 2014 - Marco Civil da Internet;

d) Law No. 13,709 of August 14, 2018 - General Law on Personal Data Protection;

e) Law No. 12,529, of November 30, 2011, which structures the Brazilian Competition Defense System;

f) Law No. 14,197, of September 1, 2021, which typifies crimes against the Democratic State of Law; and

g) Law No. 10.741, October 1, 2003, which provides for the Statute of the Elderly.

§ Paragraph 1 Freedom of expression is a fundamental right of the users of the providers dealt with in this Law, in the terms of art. 5th, clause IX, of the Federal Constitution.

Art. 4 This Law has the following objectives

I - the strengthening of the democratic process and the promotion of information diversity in Brazil;

II - ensuring the transparency of the providers in relation to their activities with the user, including the elaboration and modification of their terms of use, moderation criteria and content recommendation and identification of

advertising content;

III - the exercise of the user's right to notice, contradictory, full defense and due process in relation to content moderation;

IV - the promotion of education for the safe, conscious, and responsible use of the internet as a tool to exercise citizenship;

V - full and priority protection of the fundamental rights of children and adolescents; and

VI - the encouragement of an environment free of harassment

and discrimination. Art. 5 For the effects of this Law, it is

considered:
I - advertiser: user who pays for advertising content;

II - Automated account: account managed, wholly or predominantly, by computer program or technology to simulate, substitute or facilitate human activities;

III - content: information, processed or unprocessed, that can be used for the production and transmission of knowledge in a broad sense, contained in any medium, support or format, shared on an Internet application, regardless of the form of distribution;

IV - Search engine: internet application that allows the search by keywords of contents prepared by third parties and available on the internet, grouping, organizing and ordering the results according to relevance criteria chosen by the platform, regardless of the creation of accounts, user profiles or any other individual registration, including content indexing and except those intended exclusively for e-commerce functionalities;

V - content moderation: preparation and application of rules about accounts and content generated by third parties that imply exclusion, unavailability, reduction or promotion of scope, signaling of content, de-indexing and others with similar effect, as well as the measures employed to comply with this Law, pursuant to the regulations;

VI - profiling: any form of data processing, automated or not, to evaluate personal aspects of a natural person, aiming to classify them into groups or profiles, or for the formation of the behavioral profile or definition of their personal profile referred to in Law No. 13,709 of August 14, 2018;

VII - programmatic advertising platforms: internet application that intermediates between advertisers and companies that offer space for internet advertising, in an automated way, through algorithmic software;

VIII - provider: internet application of social networks, search tools or instant messaging, under the terms foreseen in art. 2º of this Law;

XI - platform advertising: extending or boosting the reach of content in exchange for a monetary payment or an estimated amount of money to the providers referred to in this Law;

X - user advertising: broadcasting of content in exchange for pecuniary payment or value estimable in money to the user who uses the providers referred to in this Law;

XI - social network: internet application whose main purpose is the sharing and dissemination, by users, of creation, opinions and information, conveyed by texts or image, sound or audiovisual files, on a single platform, by means of accounts connected or accessible in an articulated manner, allowing the connection between users;

XII - instant messaging: Internet application whose primary purpose is to send instant messages to certain, specified recipients, including the offer or sale of products or services and those protected by end-to-end encryption, with the exception of electronic mail services;

XIII - terms of use: contract established by the providers and the user of their services, which establishes their own content moderation rules applicable to their accounts and to content generated by them; and

XIV - user: an individual or legal entity that has an account or uses a provider.

CHAPTER II
THE LIABILITY OF THE PROVIDERS

Section I - Civil liability

Art. 6 The providers may be held civilly liable, jointly and severally:

I - for repairing the damage caused by content generated by third parties whose distribution was carried out through platform advertising; and

II - for damages arising from content generated by third parties when there is a breach of duty of care obligations, in the duration of the security protocol referred to in Section IV.

Section II - Systemic risk analysis and mitigation obligations

Art. 7 Providers must diligently identify, analyze, and assess systemic risks arising from the design or operation of their services and their related systems, including algorithmic systems.

§ Paragraph 1 The risk evaluation foreseen in the caput will consider guidelines established by regulation and will be published:

I - annually; and

II - prior to the introduction of functionalities that are likely to have a critical impact on the risks identified in accordance with this Article.

§ 2 The assessment will cover specifically in each of the providers' services and will consider systemic risks, taking into account their severity and probability of occurrence, and will include, at a minimum, the analysis of the following risks:

I - the dissemination of illicit contents in the scope of the services according to the caput of art. 11;

II - the guarantee and promotion of the right to freedom of expression, information and the press, and media pluralism;

III - concerning violence against women, racism, protection of public health, children and adolescents, the elderly, and those with serious negative consequences for the person's physical and mental well-being;

IV - the democratic rule of law and the integrity of the electoral process; and

V - the effects of unlawful or abusive discrimination as a result of the use of sensitive personal data or of disproportionate impact due to personal characteristics.

§ 3 When conducting risk assessments, providers will take into account how the following factors influence the systemic risks referred to in § 2:

I - the design of their recommendation systems and any other relevant algorithmic systems;

II - their content moderation systems;

III - the terms of use and their application;

IV - the platform advertising display systems; and

V - the influence of malicious and intentional manipulation on the service, including cases of accounts created or used for the purpose of assuming or simulating the identity of a third party to deceive the public, or exploiting the service in an automated manner.

Art. 8 The providers will adopt reasonable, proportional, and effective mitigation measures directed to the systemic risks dealt with in art. 7º :

I - adapt the design, features or operation of the services, including the systems and interfaces;

II - adapt the terms of use and the criteria and methods of application;

III - adapt the content moderation processes, including the speed and quality of processing notifications, and when necessary apply content removal, guaranteed the procedures foreseen in Chapter III;

IV - testing and adapting algorithmic systems, including prioritization and recommendation systems, for platform advertising;

V - strengthening of internal processes, resources, testing, documentation, or supervision of any of its activities;

VI - adapt the interface to provide more information to users; and

VII - take specific measures to protect the rights of children and adolescents, including adoption and improvement of age verification systems, development and promotion of tools for parental control or for reporting abuse or seeking support from children and adolescents, as provided in Chapter X.

§ 1 When the measures referred to in the caput involve the use of systems

automated systems, these should include safeguards that are appropriate and effective, especially through human supervision to ensure accuracy, proportionality, and freedom from unlawful or abusive discrimination.

§ 2 The measures implemented by providers, under the terms established in this Section, shall preserve the security of information and the protection of personal data, in accordance with Law No. 13,709, of August 14, 2018.

Art. 9 - The providers must grant, in the form of regulation and within a reasonable period of time, upon request and whenever requested, access to the data that contribute to the detection, identification, and understanding of the systemic risks generated by the providers, as well as for the evaluation of the risk mitigation measures referred to in art. 8.

Art. 10 - The providers, in the form of regulation, must present the evaluation and mitigation report of systemic risks.

Section III - Duty of Care obligations

Art. 11: ISPs must act diligently to prevent and mitigate illicit practices within the scope of their services, making efforts to improve the fight against the dissemination of illegal content generated by third parties, which may constitute:

I - crimes against the Democratic State of Law, typified in Decree-Law nº 2.848, of December 7, 1940;

II - acts of terrorism and acts preparatory to terrorism, typified by Law No. 13,260 of March 16, 2016;

III - The crime of inducing, instigating, or aiding suicide or self-mutilation, typified in Decree-Law nº 2.848, of December 7, 1940;

IV - crimes against children and adolescents foreseen in Law no. 8069, of July 13, 1990, and of incitement to crimes against children and adolescents or apology of a criminal fact or author of crimes against children and adolescents, typified in Decree-Law no. 2848, of December 7, 1940;

V - crime of racism as dealt with in art. 20, 20-A, 20-B and 20-C of Law No. 7.716, of January 5, 1989;

VI - violence against women, including the crimes set forth in Law No. 14,192 of August 4, 2021; and

VII - sanitary infraction, for failing to execute, hindering or opposing the execution of sanitary measures when under a situation of Public Health Emergency of National Importance, dealt with in art. 10 of Law No. 6.437, of August 20, 1977.

§ 1 The evaluation of compliance with the caption sentence will be made taking into account:

I - the information eventually provided in compliance with art. 9;

II - the evaluation of the reports:
a) of systemic risk evaluation, as per art. 10; and
b) of transparency, referred to in art. 23;

III - the treatment given to the receipt of notifications and complaints.

§ The evaluation will always be carried out on the set of efforts and measures adopted by the providers, not being possible to evaluate isolated cases.

Section IV - Obligations when there is imminent risk of damage

When the imminence of the risks described in art. 7 is configured, or the negligence or insufficiency of the provider's action, a security protocol may be instigated, in the form of regulation and by a grounded decision, for a period of up to 30 (thirty) days, without prejudice to other applicable legal measures, a procedure of an administrative nature whose stages and objectives shall be the object of regulation.

§ 1 The extension of the protocol, for a period of up to 30 (thirty) days, may occur when the insufficiency of less severe measures to remove the imminent risk is demonstrated, after the actions taken during the initial protocol period.

§ Once the protocol is extended, the body that issued the decision must review the need for its maintenance every 30 (thirty days), by means of an ex officio motivated decision, based on concrete facts that demonstrate the continuity of imminent risks.

Art. 13 - As of the instauration of the security protocol and due notification, the providers may be held civilly liable for damages resulting from content generated by third parties when prior knowledge is demonstrated, in the terms of art. 16.

Sole Paragraph. Providers' liability for damages arising from content generated by third parties, when there is imminent risk of damage, will be joint and several, will apply for the duration of the protocol and will be restricted to the subjects and hypotheses stipulated therein.

Art. 14: The establishment of the security protocol should point out:
I - well-founded elements that characterize the imminent risk of damage;

II - identification of impacted providers and indications that there is insufficiency or negligence in their activity;

III - the thematic delimitation of which contents generated by third parties will be liable, according to §2º of art. 7;

IV - summary text of the security protocol that should be publicized to inform the users of the respective provider;

V - duration of the protocol; and

VI - list of relevant issues that should be addressed by effective and proportionate mitigation measures by providers in their systems within the security protocol.

Art. 15 - The providers must produce specific reports of their actions involving the security protocol, according to the regulations.

§1 - Contents rendered unavailable due to the security protocol must be stored by the affected providers, for the time determined in regulation, for the purpose of further analysis.

§ Once the duration period of the security protocol is over, a report on the protocol must be published within 30 (thirty) days, based on the information offered by the providers, in the form of regulation.

§ A channel for denunciation will be created to investigate possible abuses committed within the scope of the protocol operated.

§ In case of abuse in the application of the measures foreseen in the security protocol, the providers will be subject to the sanctions foreseen in this Law.

CHAPTER III
USER NOTIFICATION AND DUE PROCESS IN CONTENT MODERATION PROCEDURES

Section I - Notification by the user

Providers must create mechanisms that allow any user to notify them of the presence, in their services, of potentially illegal content, in a justified manner.

§ The mechanism and minimum requirements for notification of contents will be defined in regulation.

§ The registration of the notification mentioned in this article configures itself as a necessary and sufficient act as proof of knowledge by the providers of the content indicated as infringing, for the purposes of the provisions of art. 13 of this law.

Section II - Content moderation and the review process

Art. 17 The content and account moderation procedure must observe the current regulations and be applied with equity, consistency, and respect for the right of access to information, freedom of expression, and free competition.

Sole Paragraph. The terms of use, as to content and account moderation, must always be guided by the principles of necessity, proportionality, and non-discrimination, including as to user access to the provider's services.

Art. 18: After applying the rules contained in the terms of use that imply content moderation, including those involving change of monetary payment or platform advertising, social network and instant messaging providers must, at least

I - notify the user who posted the content about:
a) the nature of the measure applied and its territorial scope;

b) the rationale, which must necessarily point to the clauses of its terms of use for application and the content or account that gave rise to the decision;

c) procedures and time limits for exercising the right to request a review of the decision; and

d) whether the decision was made exclusively through automated systems providing clear and adequate information regarding the criteria and procedures used for the decision, pursuant to art. 20,
§ 1, of Law No. 13,709, of August 14, 2018, when the requirements for such are met;

II - respond in a reasoned and objective manner to requests for revision of decisions and provide for their immediate reversal when equivocal.

§ 1 The code of conduct must provide for reasonable deadlines for compliance with clauses I and II of this article.

§ In case the request for revision is granted, the measures applied must be immediately revoked, and publicity must be given to the mistake found.

§ To make available, for a minimum period of six months, a separate and easily accessible channel for the formulation of complaints about contents and accounts in operation and the sending of requests to review decisions and consult the history of interactions between the provider and the user.

Section III - Publicity of content moderation actions Art. 19. The

providers referred to in this Law must:
I - create mechanisms to publicly inform the action, by the provider, of content moderation, regardless of the cause that gave rise to the moderation; and

II - keep public the identification of the judicial action that originated the moderation in contents, except for confidential proceedings.

CHAPTER IV
OF THE DUTIES OF TRANSPARENCY

Section I - Transparency on the terms of use and recommendation algorithms

The providers must make available, in an accessible manner, with clear, public and objective information, safeguarding industrial and commercial secrets, in the Portuguese language, the terms of use of their services, which must include:

I - a concise summary with the main features of the services and the main elements contained in the terms of use;

II - the types of forbidden content;

III - the age group for which they are intended;

IV - the potential risks of use;

V - explanation of the steps that the provider takes to ensure that the content complies with its terms of use;

VI - information about the means by which the user can notify the provider about possible violations of its terms of use or the presence of illegal content on its services;

VII - information about channels for receiving complaints from users and mechanisms for challenging the provider's decisions; and

VIII - information about criteria and methods of moderation in accounts and

contents and the general description of any automated systems used in this activity;

Single paragraph. When the provider offers platform advertising services, its terms of use must also inform, which contents:

I - are ineligible or may not be advertised; and

II - may give rise to a limitation on advertising.

Art. 21 - The providers' terms of use must contain the parameters used in their content recommendation systems, with the exception of commercial and industrial secrets, as well as

I - general description of the algorithms used;

II - highlighting the main parameters that determine the recommendation or targeting of content to the user; and

III - options available to users to modify the recommendation or targeting parameters.

§ The parameters referred to in item II of the caput must be able to explain why certain content is suggested to the user, include relevant criteria for determining the recommendations or directions, and how they are balanced against each other.

§ 2 Providers that use personal data for profiling for content recommendation purposes must offer the display of content not selected from such techniques and create accessible mechanisms for the user to choose between different ways of displaying, managing and targeting content on the platform.

§ The provisions of the caput apply to the targeting of platform advertising.

§4 Providers should, by default, require human action and consent from users for activation of automated playback of content, except for music content and playlists created by the user himself.

§ 5º It is forbidden to providers to stimulate the change of the standard established in § 4º.

§ 6 - Providers must adopt technical measures that make it possible to identify recommended content clearly, unequivocally, and in real time, in order to differentiate it from the content selected by the user.

Art. 22 - Providers must disclose in their terms of use the governance measures adopted in the development and use of automated systems, including those aimed at

I - security, reliability, accuracy, and illegal or abusive non-discrimination;

II - the purpose and accuracy of content moderation algorithms;

III - the systemic risk mitigation measures linked to these systems, as per art. 8 of this law.

Section II - Transparency Reports

Art. 23 - Providers must produce biannual transparency reports, made available on their electronic sites, easily accessible, machine-readable, in Portuguese, in order to inform content moderation procedures, under the terms of the regulation.

§ The periodicity of the reports may be reduced due to relevant public interest, as in cases of systematic non-compliance with the dictates of this Law, public calamity, or during election periods.

§ The reports must contain qualitative information on the procedures performed, which must include, among others, details of the account and content moderation procedures adopted, actions implemented to address illegal activities, significant changes to the terms of use and recommendation systems, and data on the teams responsible for enforcing the terms of use.

§ The reports must contain quantitative and aggregate information per operation that will enable, among other things, the determination of the number of active users and usage profiles that allow the establishment of comparison parameters in the application of the obligations provided for in this law and to assess the accuracy and precision about the quantities of complaints, notifications, and content moderation procedures, as well as those carried out in compliance with judicial measures or taken by automated means.

§ 4 Until the issue of regulations, which will detail the information described in §§ 2º and 3º , which will consider the diversity of business models, and which must integrate the transparency reports, the reports must be prepared with the information contained in the Annex of this law.

§ 5º The data and reports published must be made available with open technological standards that allow communication, accessibility and interoperability between applications and databases, guaranteeing the anonymization of personal data.

§ The transparency reports must be made available to the public within 60 (sixty) days after the end of the semester in question, and prepared in clear language, when possible using accessibility resources.

Section III - External Auditing

Art. 24 - The provider must perform and publish an annual external and independent audit to evaluate compliance with the provisions of this Law, and the regulations, which must address, at least, the following aspects:

I - the efficiency in fulfilling the obligations of systemic risk analysis and mitigation, duty of care, and when there is imminent risk of damage;

II - level of efficiency, accuracy, precision, and coverage of the mitigation measures adopted;

III - the non-discrimination or absence of bias in their account and content moderation decisions;

IV - the impacts of content moderation on content dissemination

referred to in art.11;

V - the reliability, accuracy, and unlawful or abusive non-discrimination related to the use of algorithms; and

VI - impact of algorithms on the visibility, recommendation, and ordering of journalistic content.

§ 1 Providers must share information with the independent auditors, who must account for the elements on which it was not possible to reach a conclusion and describe the third parties consulted as part of the audit;

§ Independent external audits will be considered to be organizations that

I - are independent of the providers and that they have no conflicts of interest with the providers and with any person connected to them, whether of a competitive, economic, or political nature;

II - have not provided non-audit services in connection with the audited matters to the providers, or to any person connected with them, in the twelve (12) months preceding the start of the audit, and who undertake not to provide such services in the twelve (12) month period following completion of the audit;

III - have not provided the audit services in question, nor any legal entity connected to the providers for more than ten (10) years;

IV - has not made the payment conditional on the type of result obtained in the report.

V - have proven experience in the area of risk management and risk analysis, with appropriate capacity and technical competence; and

VI - have demonstrated professional ethics, in particular, with the existence of and adherence to their respective codes of conduct.

§ Paragraph 3 Independent external audit service providers must comply with information security and confidentiality and personal data protection requirements, pursuant to Law No. 13,709 of August 14, 2018, and observe commercial and industrial secrets.

§ 4 All audits carried out under this law must adequately protect the rights and legitimate interests for which they are intended, and may not require access that violates the protection of personal data, trade secrets, and other confidential information of the providers and any other parties involved, including the recipients of the service.

Section IV - Access to Research

Art. 25 - The providers must make feasible the free access of scientific, technological and innovation institutions to disaggregated data, including by means of application programming interface, for academic research purposes, observing commercial and industrial secrets, anonymization and protection of personal data pursuant to Law nº 13.709 of August 14, 2018 and as regulated.

Sole paragraph. The provisions of the caput include access to information about the algorithms used in account and content moderation, prioritization, segmentation, recommendation and display of content, advertising of

platform and boosting, and sufficient data on how these algorithms affect the content viewed by users.

CHAPTER V
THE DUTIES REGARDING DIGITAL ADVERTISING

Art. 26: The providers that offer platform advertising must identify it, so that the user responsible for the boost or the advertiser are identified.

§ 1 Providers must offer relevant information, directly and easily accessible from the advertisement, about the main parameters used to determine the recipient of the platform advertising display and how to change these parameters.

§ The provisions of the caput also apply to programmatic advertising and user advertising platforms, which must be publicly informed by the beneficiary and
identified to other users by the provider in an unambiguous way.

§ 3 The provider must provide a mechanism for user publicity to be publicly informed to other users.

§ 4º Programmatic advertising providers and platforms must submit information, updated at least every six months, containing the entire repository of ads and boosted content and including among these the full content, the information that allows the identification of the person responsible for the payment, the general characteristics of the contracted audience and the total number of recipients reached, as well as additional and specific criteria to be stipulated in regulation.

§ 5º The information mentioned in § 4º must be made available with open technological standards that allow communication, accessibility and interoperability between applications and databases.

Art. 27 - The provider and the programmatic advertising platforms must require the identity, through the presentation of a document valid in the national territory, of all platform advertisers:
I - of the natural or legal person on whose behalf the platform advertising is presented;

II - of the individual or legal entity paying for the platform advertising, if different from the person referred to in item I.

Sole Paragraph. Except as provided in art. 26, the identification of the platform's advertising contractor must be kept confidential by the providers, and may be required by court order.

Art. 28 - The provider that offers platform advertising must make available mechanisms to provide users with historical information on the advertising content with which the account has had contact in the last 6 (six) months, detailing information regarding the criteria and procedures used for profiling that were applied in each case.

Art. 29 - The commercialization of platform advertising for disclosure by providers headquartered abroad must be performed and recognized by their representative in Brazil and in accordance with the legislation governing Brazilian advertising, when intended for the domestic market.

Art. 30 The sharing of personal data of users of the providers with third parties, when they have as their exclusive objective the direct or indirect exploitation in the market in which it operates or in other markets, must observe Law No. 13,709, of August 14, 2018 and with the provisions of art. 36 of Law No. 12,529, of November 30, 2011.

CHAPTER VI
COPYRIGHT AND RELATED RIGHTS

Art. 31 - The contents protected by copyright and related rights used by the providers, including those offering on-demand content and produced in any format that includes text, video, audio or image, will give rise to remuneration to their holders by the providers, including the application providers offering on-demand content, in the form of regulation by the competent organ, which will dispose about the criteria, form to assess the values, negotiation, conflict resolution, transparency and the valorization of the national, regional, local and independent content.

§ Paragraph 1 The caput covers musical and audiovisual content, without prejudice to other content protected by Law n. 9.610, of February 19, 1998, guaranteeing the valorization of national, regional, local and independent content.

§ The owners of the protected contents mentioned in the caput should preferably exercise their rights through copyright collective management associations, which will negotiate with the providers the values to be practiced, the model and term of remuneration, under the terms of the regulation, observing the provisions of §15 of art. 98, of Law 9610, of February 19, 1998.

§ In the process of defining the criteria and the way to measure the remuneration referred to in the caput, the totality of the revenue, including advertising, generated in benefit of the providers, and including the application providers offering on-demand content, by virtue of content consumed in Brazil or by virtue of content produced by Brazilian citizens, will be considered.

§ 4 It is forbidden to providers, including application providers offering on-demand content, to frustrate or reduce, by any means, the remuneration of copyrights and related rights due under the terms of this Article.

§ 5 - The eventual accounting of revenues described in § 4 at a tax domicile abroad does not constitute a legitimate reason to reduce or frustrate the payment foreseen in this article, even in cases in which such an accounting operation may be considered lawful from a strictly tax point of view.

§ 6 - The providers, including application providers offering on-demand content must adopt mechanisms to identify and neutralize the action of automated accounts that artificially distort rankings and playlists.

§ 7 - In the case of providers, including application providers offering on-demand content, it is forbidden to artificially increase or reduce, without informing the user, the frequency of use of specific works or phonograms in order to favor, in the recommendation systems based on algorithms, the remuneration to a company belonging to the same economic group, to a partner, controlling company or affiliate of the platform, as well as to the company that has entered into a commercial agreement with the platform".

CHAPTER VII
OF THE JOURNALISTIC CONTENTS

Art. 32 - Journalistic content used by providers produced in any format, including text, video, audio, or image, will give rise to remuneration to journalistic companies, in the form of regulation, which will dispose of the criteria, the way to assess values, negotiation, conflict resolution, transparency, and the valorization of national, regional, local, and independent professional journalism.

§ 1 The remuneration referred to in the caput should not burden the end user who accesses and shares the journalistic content without economic purposes.

§ A legal entity, even an individual one, established for at least 24 (twenty-four) months, which produces original journalistic content in a regular, organized, and professional manner and which maintains the physical address and editor in charge in Brazil, will be entitled to the remuneration foreseen in the caput.

§ 3 The agreement between the application provider and the journalistic company is free, guaranteed the collective negotiation by the legal entities foreseen in § 2, including those belonging to the same economic group, with the providers regarding the values to be practiced, the remuneration model and term, observing the regulation.

§ The regulation will provide for arbitration in cases where negotiation between ISP and news company is unfeasible.

§ 5 The regulation referred to in this article must create mechanisms to guarantee equity between providers and journalism companies in negotiations and conflict resolutions, without prejudice to companies classified as small and medium-sized, in the form of regulation.

§ 6 - The provider cannot promote the removal of journalistic content made available with the intention of exempting itself from the obligation dealt with in this article, except in the cases foreseen in this Law, or by specific judicial order.

§ 7º The Administrative Council for Economic Defense - CADE will restrain acts of infraction to the economic order of the application provider that abuses its dominant position in the negotiation with journalistic companies.

CHAPTER VIII
OF THE ACTION OF THE PUBLIC POWER

Art. 33 - Accounts maintained in social networks indicated as institutional by members of the Federal, State and Municipal Public Administration, directly or indirectly, and by the following political agents are considered of public interest:
I - holders of elective mandates in the Executive and Legislative Branches of the Union, the States, the Federal District, and the Municipalities;

II - occupying, in the Executive Branch, the positions of
a) Minister of State, Secretary of State, Municipal Secretary or alike; and
b) President, Vice-President and Director of the entities of the indirect Public Administration of the Union, the States, the Federal District and the Municipalities;

§ Paragraph 1 The holders of the accounts mentioned in the head of this article cannot restrict the visualization of their publications.

§ The decisions by providers that constitute illicit or abusive active intervention in accounts of public interest authorize the filing of a lawsuit for their restoration, and the Judiciary must oblige providers to restore them within 24 (twenty-four) hours, in cases where it is proven that their operation conforms to fundamental rights and the principles of legality, impersonality, morality, publicity, and efficiency.

§ If the political agent has more than one account in a platform, he must indicate the one that officially represents his mandate or position to the respective regulatory body, the others being exempt from the obligations of this article.

§ The other accounts referred to in § 3 will be considered as being of public interest, even if they do not officially represent the political agent, if they contain, predominantly, official manifestations proper to the office of these agents.

§ 5 The regulatory body referred to in § 3 will forward the list of accounts of public interest to social network providers and private messaging providers within 60 (sixty) days of the agent taking office or creating the account, whichever occurs first.

§ 6º The material parliamentary immunity, in the form of art. 53 of the Federal Constitution, extends to the contents published by political agents on platforms maintained by social network providers and private messaging.

Art. 34 - The entities and bodies of the Public Administration, direct or indirect, must include in their transparency portals the following data about the contracting of platform advertising:

I - value of the contract;

II - data from the contracted company and form of contracting;

III - campaign content;

IV - mechanism for the distribution of resources;

V - criteria for defining the target audience;

VI - list of the pages, applications, games, channels, websites and other media where such resources have been applied; and

VII - number of appearances and value applied to the sum of the appearances.

Art. 35 - The Public Administration will not allocate public resources for publicity in electronic sites and accounts in social networks that promote, recommend or direct to speeches destined to the illicit acts mentioned in the caput of art. 11.

§ It is forbidden for the Public Administration to contract advertising from providers that are not constituted according to the Brazilian legislation.

§ 2 All and any communication of an advertising nature disseminated by the public administration at the federal, state, and municipal levels must be registered in a repository on the respective electronic site, according to the regulations.

Art. 36 - The Public Administration must make available and specify the information about resources invested in publicity destined to means of

communication, including Internet application providers.

Art. 37 - Any disciplinary punishment or act practiced by a hierarchical superior that causes damage to a civil public servant due to lawful content shared by him privately, outside the exercise of his functions, constitutes an unlawful act, punishable under criminal and administrative law.

CHAPTER IX
PROMOTING EDUCATION FOR THE SAFE USE OF THE INTERNET

Art. 38 The fulfillment of the constitutional duty of the State in the provision of education, at all levels of education, includes:

I - training, integrated with other educational practices, for the safe, aware, and responsible use of the Internet applications referred to in this Law, including campaigns to avoid misinformation;

II - the development of critical thinking, research skills, ethics, and respect for pluralism of opinions;

III - the development of skills for argumentation, reflection, and critical analysis;

IV - guaranteeing and teaching about the right to access to information;

V - raising awareness of the role of privacy, personal data protection, and informational self-determination, as well as the means to ensure them;

VI - the rapid promotion of digital literacy; and

VII - the training of teaching professionals to attend to the previous items.

§ 1º The Union, the States, and the Municipalities should make efforts, including budgetary efforts, to expand and qualify the participation of children, adolescents, and youth in school practices that promote media education according to the guidelines set forth in the Common National Base provided for in art. 26 of Law no. 9.394, of December 20, 1996, in order to develop in the students a set of abilities to access, analyze, create, and participate in a critical way in the informational and media environment in all its formats and to develop their communication potentials in the several media, based on the abilities of conscious interpretation of information, active production of contents, and responsible participation in society.

§ The actions must be developed in an articulate manner with the strategies foreseen in the National Policy for Digital Education, in the terms of Law 14.533, of January 11, 2023, and the sources of resources provided in art. 11 of this law, can be used for the implementation of actions that observe the purposes mentioned in this article.

CHAPTER X
PROTECTION OF CHILDREN AND ADOLESCENTS

The services of providers accessible by children and adolescents must have as a parameter of their services the best interests of the child and

adopt appropriate and proportionate measures to ensure a high level of privacy, data protection and security, as defined by Law No. 8,069 of July 13, 1990 and Law No. 13,709 of August 14, 2018.

Single paragraph. Providers must create mechanisms to actively prevent the use of services by children and adolescents, whenever they are not developed for them or are not appropriate to meet the needs of this public.

Art. 40 - The creation of behavioral profiles of users, children and adolescents, from the collection and processing of their personal data, including those obtained in age verification processes, as well as group and collective data, for the purpose of targeting advertising, is forbidden.

Sole Paragraph. For the adequate fulfillment of the provisions in the caption of this article, the providers must adopt reasonable technical measures to verify the age of their users, observing their right to privacy and personal data protection.

CHAPTER XI
PROVIDERS OF INSTANT MESSAGING SERVICES

Section I - About the duties of instant messaging services

The services of instant messaging providers are obliged to guarantee privacy and to design their platforms to limit the mass distribution of contents and media, and to this end they must

I - limit, in accordance with the code of conduct, the forwarding of messages or media to multiple recipients;

II - determine that broadcast lists may only be forwarded and received, in any event, by persons who are identified, at the same time, in the contact lists of senders and recipients;

III - institute a mechanism to verify the user's prior consent for inclusion in message groups, mailing lists, information dissemination channels open to the public or equivalent user grouping mechanisms, except in the case of emergency, state of public calamity and similar circumstances, in accordance with the regulations; and

IV - disable by default the authorization for inclusion in groups and mailing lists or equivalent mechanisms for forwarding messages to multiple recipients.

§ 1 The provisions of Chapters II and III of this law apply to broadcasting channels open to the public offered by instant messaging providers, with the exception of modalities not open to the public, including those protected by end-to-end encryption.

§ Instant messaging providers must create solutions to identify and prevent external mass distribution mechanisms.

§ 3º Code of conduct shall establish obligations for instant messaging providers to take other preventive measures to curb mass distribution of content within their services and to promote the established in the caput.

Art. 42 - A court order may order the instant messaging providers to preserve and make available sufficient information to identify the first account reported by other users when the sending of illicit contents is involved.

§ 1 The court order referred to in the caput will only be admitted:

I - if determined ex officio or at the request of the police authority or the Public Prosecutor's Office;

II - for the sole purpose of evidence in criminal investigation, in criminal procedural instruction and in electoral investigation and instruction; and

III - with specific identification of the illicit content that gave rise to the investigation, proven through electronic copy.

§ The information preservation order mentioned in the head of this article is limited to information sufficient to identify the first account reported by other users when the illicit content that gave rise to the investigation was sent, and its term cannot exceed six months.

Art. 43: Instant messaging providers that offer account services intended for commercial use to customers that facilitate automated and large-scale triggering to multiple users must develop measures to ensure that the service is used strictly for institutional or commercial purposes, the promotion of commercial products or services, or the provision of a public service.

§ 1 - The commercial accounts mentioned in the caput in instant messaging services must guarantee the publication of information that identifies the sender of the message.

§ Instant messaging providers that offer commercial accounts must require from their users, whether individuals or companies, a conscious and unequivocal statement that the commercial application is not to be used for electoral and partisan propaganda purposes, nor to distribute any content unrelated to institutional and commercial purposes.

§ If the instant messaging service provider is aware of the forwarding of messages and media that do not fall within the scope of the commercial service, the account must be blocked.

CHAPTER XII
OF THE JUDICIAL AND INVESTIGATION PROCEDURES

Art. 44 Judicial decisions that determine the immediate removal of illicit content related to the practice of crimes to which this Law refers, must be complied with by the providers within twenty-four hours, under penalty of a fine of R$ 50,000.00 (fifty thousand reais) up to R$ 1,000,000.00 (one million reais), per hour of non-compliance, as of the end of the twenty-fourth hour after the notification has been received.

Sole paragraph. The fine provided for in the caput may be applied in three times its amount in cases involving platform advertising.

Art. 45: When the ISP becomes aware of information that raises suspicion that a crime involving threat to life has occurred or may occur, he must immediately inform the competent authorities of his suspicion.

Art. 46 - The providers must keep, for a period of 6 (six) months, as of the removal or deactivation:
I - content that has been removed or to which access has been disabled as a consequence of the duties established by this Law or by court decisions, as well as any related data and metadata removed; and

II - the respective application access data, such as the access log, Internet protocol address, including the source ports, in addition to registration data, telematic data, other user records and information that may be used as evidential material, including those related to the form or means of payment, if any.

§ At the formal request of the competent authorities, or due to a court decision, the term in the caption can be extended, as long as necessary within the scope of an administrative or judicial process in progress, until its respective conclusion.

§ 2 Providers must ensure that the illicit content and related data are subject to appropriate technical and organizational procedures, including ensuring the chain of custody of the evidence.

CHAPTER XIII
SANCTIONS

Art. 47 - The providers, due to the infringements committed against the norms foreseen in this Law, are subject to the following administrative sanctions, applicable separately or cumulatively:
I - warning, with an indication of the deadline for adopting corrective measures;

II - daily fine, observing the total limit referred to in item lll;

III - a simple fine, of up to 10% (ten percent) of the economic group's billing in Brazil in its last fiscal year or, in the absence of billing, a fine of R$ 10.00 (ten reais) up to R$ 1,000 (one thousand reais) per registered user of the sanctioned provider, limited, in total, to R$ 50,000,000.00 (fifty million reais), per infraction;

IV - publication of the decision by the offender;

V - prohibiting the processing of certain databases; and

VI - temporary suspension of activities.

§ 1 - After an administrative procedure that allows for the opportunity of full defense, the sanctions will be applied gradually, separately or cumulatively, according to the peculiarities of the concrete case and considering the following parameters and criteria:
I - the gravity and nature of the offenses and the possible violation of rights;

II - the good faitḥ of the offender;

III - the advantage gained by the offender, when it is possible to estimate it;

IV - the economic condition of the offender;

V - the recidivism;

VI - the degree of damage;

VII - the cooperation of the offender;

VIII - the prompt adoption of corrective measures; and

IX - the proportionality between the seriousness of the misconduct and the intensity of the sanction.

§ Prior to or during the administrative proceeding of Paragraph 1, preventive measures may be adopted, including coercive fines, observing the total limit referred to in item III of the caput, when there is evidence or well-founded fear that the provider:
I - causes or may cause irreparable damage or damage that is difficult to repair; or

II - render the result of the process ineffective.

§ Paragraph 3 The provisions of this article do not replace the application of other administrative, civil or criminal sanctions defined in Law No. 8,078 of September 11, 1990, Law No. 13,709 of August 14, 2018, and specific legislation.

Art. 48. Sanctions will not be applied to specific content moderation processes on the providers' own initiative and in accordance with their terms of use, except in case of systematic failure to comply with the obligations foreseen in Chapter III.

Art. 49 - The proceeds from the collection of the fines levied based on this Law, whether or not recorded as collectible debt, will be destined to the Fund for the Defense of Diffuse Rights provided for in art. 13 of Law nº 7.347, of July 24, 1985, and Law nº 9.008, of March 21, 1995.

CHAPTER XIV
OF THE CRIME IN KIND

Art. 50 - Promoting or financing, personally or through third parties, through the use of an automated account and other means or expedients not directly provided by the internet application provider, the mass dissemination of messages that contain a fact that is known to be untrue, that is capable of compromising the hygiene of the electoral process, or that may cause damage to physical integrity and is subject to criminal sanction.
Penalty: imprisonment, from 1 (one) to 3 (three) years, and a fine.

CHAPTER XV
REGULATION OF THE PROVIDERS

Art. 51 The following shall be the attributions of the Brazilian Internet Steering Committee (CGI.br), in addition to those provided for by Laws No. 12,965 of April 23, 2014, and No. 13,853 of July 8, 2019:
I - conduct studies, opinions, and propose strategic guidelines on internet freedom, responsibility, and transparency;

II - conduct studies and debates to deepen the understanding of disinformation, and propose guidelines for combating it, in the context of the internet and social networks;

III - provide guidelines for the development of a code of conduct for providers of social networks, search engines, and instant messaging to ensure the principles and objectives set forth in arts. 3 and 4, including obligations for instant messaging services to take preventive measures to curb the mass dissemination of content and to address misinformation in the context of the internet and social networks;

IV - validate the codes of conduct prepared as per item III of this article;

V - conduct studies on the account and content moderation procedures adopted by social network providers, as well as suggest guidelines for their implementation;

VI - provide guidelines and subsidies for the terms of use of social networking and instant messaging service providers;

VII - organize, on an annual basis, a national conference on Internet freedom, accountability and transparency;

VIII - publish the list of providers that fit into the provisions of art. 2º of this law;

IX - issue recommendations prior to the eventual opening of administrative proceedings in case of insufficient information contained in the transparency reports or unsatisfactory assessment by the independent audit.

X - issuing guidelines and criteria for the establishment of the security protocols referred to in this Law;

XI - issuing guidelines and requirements for the analysis of systemic risks referred to in this Law; and

XII - analyze the providers' systemic risk assessment reports.

Sole paragraph. The multisectorial composition of the CGI.br is guaranteed in order to fulfill its competencies, with the participation of the Public Authorities, the business sector, the third sector, and the technical-scientific community.

Art. 52 - The providers must prepare a code of conduct based on guidelines defined by CGI.br, including measures to guarantee the purposes of this law, with the creation of qualitative and quantitative indicators.

§ 1 The code of conduct must be formulated within six months after the guidelines are issued and presented to the CGI.br for validation.

§ The code of conduct and the indicators foreseen in the caput must be public, except when publicity compromises the security of its application and the services offered by the application providers.

§ Providers must make publicly available a space for the presentation of reports of violations of the policies and measures contained in the code of conduct, or add this possibility to their tools for receiving reports.

Art. 53 - The providers will be represented by a legal entity in Brazil, whose

Identification and information will be easily accessible on the internet service providers' sites, and these representatives must make user registration information available to the authorities that have legal authority to request it, under the terms of this law.

Sole paragraph. The representation referred to in the caput must have full powers to
I - respond in the administrative and judicial spheres;

II - provide the competent authorities with information concerning the operation, the proper rules applicable to the expression of third parties and the marketing of the provider's products and services;

III - comply with judicial determinations; and

IV - respond and comply with any penalties, fines, and financial implications that the company may incur, especially for noncompliance with legal and judicial obligations.

CHAPTER XVI FINAL PROVISIONS

Art. 54 - Items VI and VIII of art. 5, art. 13 and art. 15, all of Law No. 12,965, of April 23, 2014, shall take effect with the following wording:

"Art. 5º
.....

.....
.....

VI - connection log: the set of information referring to the start and end date and time of an internet connection, its duration, the IP address and the logical port used by the terminal for sending and receiving data packets;

.....
.....

VIII - records of access to internet applications: the set of information regarding the date and time of the start and end of access to a given internet application from a given IP address and logical port" (NR)

"Art.13.....

.....

§ The police or administrative authority, or the Public Prosecutor's Office, may request in a precautionary manner that the connection records and personal registration data be kept for a period longer than that established in the preamble.

.....

§ 5. In any hypothesis, the availability to the requester of the records referred to in this article and of the personal registration data must be preceded by judicial authorization, as provided in Section IV of this Chapter, and the availability of registration data must comply with art. 10, § 3, of this Law.

.....

§ The requests mentioned in § 2 must be made within the scope of administrative or judicial proceedings in progress and specify the individuals whose data is being requested and the information desired; collective requests that are generic or non-specific are prohibited." (NR)

"....

....

§ The police or administrative authority or the Public Prosecutor's Office may request in a precautionary manner that the records of connection, of access to internet applications, personal registration data or other information identifying the user or terminal related to the record of access to the existing application be kept, including for a period longer than that provided in the caput, in compliance with the provisions of §§ 3 and 4 of art. 13. 3 In any hypothesis, the availability to the applicant of the records dealt with in this article must be preceded by judicial authorization, as provided in Section IV of this Chapter, and the availability of registration data must observe the provisions of art. 10, § 3, of this Law.

...."(NR)

Art. 55 - Art. 19 of Law No. 12,965, dated April 23, 2014, shall come into force with the following paragraph:

"Art.
19....

....

§ 5º The civil liability foreseen in Article 6 of the Brazilian Law of Freedom, Responsibility and Transparency on the Internet constitutes an exception to the provisions of the caption of this article." (NR)

Art. 56 Art. 21 of Law No. 12,965, dated April 23, 2014, shall come into force with the following wording:

"The Internet application provider that makes available content generated by third parties will be held subsidiarily liable when, after receipt of notification by the participant or his legal representative, fails to diligently promote, within the scope and technical limits of its service, the unavailability of content that:

I - violates intimacy, resulting from the disclosure of scenes of nudity or sexual acts of a private nature without the authorization of its participants; or

II - contains images or representations of violence or scenes of sexual exploitation or abuse involving children or adolescents, under the terms of Law No. 8069 of July 13, 1990.

...."
(NR)

Art. 57 - Law Nº 9.504, of September 30, 1997 will come into effect with the following alterations:

"Art.26 .....
.....
XVI - expenses related to the contracting of
data processing;
....."(NR)

"Art. 28 .....
.....
§
4º.....
.....
III - the registration of its data processing activities, pursuant to Article 37 of Law 13,709 of August 14, 2018.
....."(NR)

Art. 58 Art. 319 of the Code of Criminal Procedure - Decree-Law nº 3.689, of October 3, 1941 shall come into force with the following wording:

"Art. 319. They are precautionary measures different from prison:

.....

X - removal or blocking of content, suspension of profile or account, or prohibition of Internet access.

....."(NR)

Art. 59 - Within a period of 5 (five) years as of the publication date of this Law, its revision will be promoted, based on the evaluation of the fulfillment of the principles, objectives, and responsibilities of this Law, as well as the assessment of the effectiveness and accuracy of the transparency measures and reports mentioned in arts. 10 and 23.

Art. 60 This Law goes into effect on
I - 12 (twelve) months, as of the date of its publication, as to arts. 7º to 10 and 23 to 25;

II - 90 (ninety) days, as of the publication date, for articles 12 to 15, 20 to 22, 26 to 30, 32, 38, 39, 40 and 44 to 46; and

III - on the date of its publication, for the other devices.

ANNEX

1. Information to be contained in the qualitative report referred to in art. 23, § 2º :
1.1 Detailing of the procedures adopted and the way to comply with the obligations set forth in this Law, as well as modifications that occurred in the period;
1.2 Qualified description of steps taken, new tools or other actions by the third-party content digital platforms to eliminate criminal activities from the platform;
1.3 Information about significant changes made to the systems for recommending, organizing and prioritizing journalistic and news content, the objectives and justifications;
1.4 General description of the algorithmic systems used and the main parameters

that determine the targeting, recommendation, or display of content to users, including:

a) the reasons for the relative importance of such parameters;

b) the options available to users to modify or influence the recommendation parameters and aggregate data on user adherence to the different parameters;

c) the most significant criteria in determining the information recommended to users and how they are balanced against each other;

d) the goals that the system is designed to achieve and the evaluation of the system's performance against these goals; and

e) what kind of content or elements the algorithmic systems are optimizing and prioritizing for content display on the platform;

1.5 Content-specific rating decisions and moderations with the type of content that the platform downgrades, discourages or excludes, including changes made in the period; and

1.6 Content displayed as results of the recommendation system at subgroup levels, in order to demonstrate how it behaves towards each demographic group;

1.7 Criteria and methodologies used to provide information to users about modifications of own policies and terms of use and about decisions of active intervention of the platform and its applications on content or account; and

1.8 The criteria, methodologies and metrics for measuring the reach of platform advertising, subject to independent verification and audit.

2. Aggregate information that should contain the quantitative report referred to in art. 23, § 3º :

2.1 Total number of users accessing the providers from connections located in Brazil in the analyzed period;

2.2 Granularized information about the quantity of content generated by its users, average time of use, and other metrics indispensable to establish parameters of comparison for the application of the obligations foreseen in this law.

2.3 Total number of reports and notifications made by users and the classification of their content by category of violation of the terms of use policies and national legislation;

2.4 Total number of measures applied to accounts and content, as per the caput, adopted due to compliance with the providers' own terms and policies of use and compliance with this Law, segmented by rule applied and by type of measure adopted;

2.5 Total number of requests for review submitted by users to measures applied to accounts and content, according to the caput, due to the providers' own terms and policies of use and compliance with this Law, as well as measures reversed after review of appeals, segmented by rule applied and type of measure adopted;

2.6 Proportion of decisions reversed on accounts and content, after review requests, segmented by violation category and decision type, including segmentation of decisions adopted in an automated manner and the average time between review requests and reversal of decisions;

2.7 Total number of measures applied to accounts and content adopted due to compliance with court order, respecting the information under judicial secrecy;

2.8 Number of notifications handled by automated means;

2.9 Average time between the detection of irregularities and the adoption of measures regarding the accounts and contents referred to in items 2.2, 2.3 and 2.4;

2.10 General characteristics of the staff involved in the enforcement of terms of use and policies in relation to content generated by third parties, including number of people involved in the activity, hiring model, as well as statistics on their working language, qualifications, indicative of diversity, demographic attributes, and nationality;

2.11 Total number of signaling measures, removals or suspensions that were reversed by the provider;

2.12 Aggregate information about the comparative reach of content identified as irregular by the ISP in relation to the other content in circulation during the period;

2.13 Data related to engagements or interactions with content that was identified as irregular, including number of views and

shares and reach;
2.14 The criteria, methodologies and metrics used by its automated systems in monitoring and enforcing its own policies and terms of use;
2.15 In the case of automated moderation measures, general information about their operating criteria, degree of accuracy, distinguishing between degree of precision and coverage, and mechanisms for monitoring, measuring, and controlling bias;
2.16 Information about the employment and operation of automated systems, including the basis of operation and training of algorithms and the analysis of their impact on the circulation, availability, promotion, downscaling or removal of content;
2.17 Update of the own policies and terms of use made in the semester, the date of the modification and the general justification for its change;
2.18 Total number of measures applied to the accounts referred to in art. 33 of this Law, segmented by rules applied, by methodology used in the detection of non-compliance and in what proportion, and by type of measure adopted; and
2.19 Complete information about the application of the code of conduct and measures determined by the independent regulatory body, including its performance from metrics agreed with the regulatory body and the amount of investment made.

Hall of Sessions, on of 2023.

Deputy ORLANDO SILVA
Rapporteur

2023_5517