Licks
ATTORNEYS

BR Internet Act – remarks on the Supreme Court ruling

Jul.28, 2026

01 INTRODUCTION

02 PRELIMINARY ANALYSIS ON THE TRIAL ON THE UNCONSTITUTIONALITY OF ARTICLE 19 OF THE BR INTERNET ACT

This document is a preliminary analysis prepared, it reflects our initial assessment of the Brazilian Supreme Court's ruling on the unconstitutionality of Article 19 of the BR Internet Act, as of July 28, 2025.

We are continuing to study the decision and its regulatory implications in greater depth, and the conclusions expressed herein may evolve as new information and/or clarification become available.

We are available to discuss the impacts of the ruling in more detail and possible strategies to be adopted from now on.

Best regards,

03 EXECUTIVE SUMMARY

On June 26, 2025, the Brazilian Supreme Court ("STF") concluded the trial on the constitutionality of Article 19 of the Brazilian Internet Act (Law #12,965/2014 – "MCI"), ruling the Article partially unconstitutional.

In a groundbreaking decision, the STF provided new interpretation to Article 19, reshaping the original civil liability regime of internet service providers ("ISPs") for damages arising from user-generated content, which now vary depending on the content involved:

- Notice-and-takedown: content must be taken down upon a mere notification, under penalty of the ISP being deemed liable for the damages caused by them. This is now the general rule, applicable to content/accounts that portray crimes or illicit acts and replicated content involving crimes against honor that has already been deemed as infringing by a court order;
- Judicial-takedown (original Article 19 rule): platforms will only be held liable after non-compliance with a specific court order determining the content removal. This now applies to content involving crimes against honor only;
- Proactive removal: content must be taken down proactively, regardless of notification or court order. This applies to content involving serious crimes – in which case failure to adopt adequate measures will be considered a systemic flaw and will subject ISPs liable for damages arising from such content; and paid advertisements and promoted content – in which case ISPs may only be exempted from liability when there is proof that they diligently and timely took down the infringing content.

This new civil liability regime does not apply to *(a)* e-mail service providers, *(b)* providers primarily offering closed meetings by video or voice, *(c)* providers of instant messaging services, exclusively with regard to interpersonal communications (also called private messaging service providers), protected by the confidentiality of communications, and *(d)* marketplaces.

Besides the changes in the liability regime, the ruling also imposed several novel regulatory requirements to ISPs operating in Brazil, aimed at strengthening their responsibility and accountability, such as establishing self-regulatory mechanisms, improving transparency, enhancing user support, and ensuring local legal representation.

This decision marks a turning point in Brazil's digital regulatory landscape. ISPs will now need to strengthen content moderation practices or risk civil liability. Compliance efforts will be essential moving forward.

Context about the trial

What is the MCI. The Brazilian Internet Act was enacted in 2014 following intense public debate and engagement from civil society. At the time, it was recognized as a pioneering legal framework and an international benchmark for internet regulation.

Designed to safeguard the exercise of citizenship in digital environment, promote diversity and freedom of expression online, and protect privacy and personal data, the MCI sets out the core principles governing internet use in Brazil, creating rights for users and obligations for ISPs. Among its main dispositions, it establishes, in its Article 19, ISPs' general civil liability regime for third-party content.

What is the Article 19 original rule. Article 19 of the Brazilian Internet Act, in its original version, establishes that ISPs may only be held liable for damages arising from third-party content after failing to comply with a specific court order mandating its removal (judicial-takedown), subject to limited exemptions under the notice-and-takedown regime.

What was under discussion. In the past years, Brazilian courts have been inundated with lawsuits involving the takedown of allegedly infringing content and the resulting civil liability. As the volume and complexity of these cases increased, courts began to question the legality and potential unconstitutionality of Article 19 of the MCI. This growing judicial scrutiny ultimately led to the submission of several cases to the Supreme Court, which was tasked with determining whether the "safe harbor" granted by Article 19 violates the Brazilian Constitution.

The context of the trial. The relation between digital platforms and the Brazilian government (including the Judiciary) has grown increasingly tense in recent years.

A series of episodes – such as the shocking instances of criminal activities happening in social media, the use of fake news and online platforms to disrupt electoral processes and undermine public institutions, and certain platforms' refusal to comply with court orders – has prompted both the government and a significant segment of public opinion to call for tighter regulation and greater accountability of ISPs.

This pressure led to the introduction of several proposals in Congress aiming to impose stricter regulations on ISPs and social media platforms. The most notable was Bill #2,630/2020, popularly referred to as the "Fake News Bill". However, due to a lack of political consensus and support, these initiatives stalled.

In parallel, the Supreme Court has taken a firm stance in investigating and holding digital platforms accountable. Within this context, the Court began to impose increasingly stringent measures to assert its authority. Platforms' resistance to comply with the STF's demands has resulted in progressively stricter measures, ultimately leading, in some cases, to the blocking of their services. This was the background for the bans imposed on Telegram, X (formerly Twitter), and Rumble, recently ordered by the STF after they failed to comply with orders from the court.

During the trial of the case at hand, the Supreme Court urged the Congress to pass new

regulations imposing stricter rules for ISPs. In the face of continued legislative inaction, however, the Court proceeded with adjudicating the case, ultimately redefining the interpretation of Article 19, reformulating the civil liability regime and imposing new obligations on ISPs.

The Ruling

In a groundbreaking decision, the Supreme Court deemed Article 19 partially unconstitutional, and provided new interpretation to it, summarized in a Thesis binding to all Brazilian courts. This Thesis reshaped the Article 19 civil liability regime and imposed novel several regulatory requirements to ISPs operating in Brazil.

The STF explicitly stated that current internet legislation lacks sufficient safeguards for constitutionally protected rights and democratic principles. Congress was criticized for failing to create new regulations, and the Court declared that, until new legislation is passed, and except for the application of specific provisions of the electoral legislation, ISPs' civil liability for damages arising from third-party content will vary depending on the content involved, as follows:

Type of contente	Regime
Content involving crimes and illicit acts in general; and non-authentic accounts	ISPs will be held liable if they do not remove infringing content after a mere notification requesting to take it down *(notice-and-takedown).*
Content involving crimes against honor	ISPs will only be held liable after non-compliance with a specific court order determining the removal of the infringing content *(judicial-takedown).*
Paid advertisements and promoted content or artificial distribution networks (chatbots or robots)	ISPs are presumptively liable for damages arising from such content, regardless of notification or court order, and may only be exempted when there is proof that they diligently and timely took down the infringing content.
Content involving serious crimes[1]	ISPs have a duty of care to takedown content involving serious crimes. Failure to adopt adequate measures in this regard will be considered a systemic flaw and will subject ISPs liable for damages arising from such content. Isolated instances of illicit content are insufficient to trigger civil liability under this item. In this case, the *notice-and-takedown* regime shall apply.

[1] For the effect of the ruling, the following are considered serious crimes: (a) anti-democratic conducts and acts aiming at the violent abolition of the Democratic Rule of Law or disruption of the electoral process; (b) terrorism or preparatory crimes for terrorism; (c) inducement, instigation, or assistance to suicide or self-mutilation; (d) incitement to discrimination on the basis of race, color, ethnicity, religion, national origin, sexuality, or gender identity, as well as homophobic and transphobic conduct; (e) crimes committed against women because of their sex, including content that propagates hatred of women; (f) sexual crimes against vulnerable people, child pornography, and serious crimes against children and adolescents; and (g) human trafficking.

These rules do not apply to *(a)* e-mail service providers, *(b)* providers primarily offering closed meetings by video or voice, *(c)* providers of instant messaging services, exclusively with regard to interpersonal communications (also called private messaging service providers), protected by the confidentiality of communications. These services remain under the original Article 19 civil liability regime (*judicial-takedown*). Marketplaces' liability regime is as provided by consumer legislation.

In addition, the ruling has also established several regulatory requirements for ISPs operating in Brazil, such as:

- Develop self-regulation that includes notification systems, due process, and annual transparency reports;
- Offer accessible customer service channels for both users and non-users;
- Publicly disclose and regularly review their terms of service and content policies;
- Establish and maintain local presence and a representative in the country, with clear and accessible contact information published on their websites.

In addition to the description provided in this chapter, please see the complete transcription of the Thesis established by STF, along with our comments, in the Appendix.

Possible impacts on ISPS

This decision marks a turning point in Brazil's digital regulatory landscape. ISPs will now need to strengthen content moderation practices or risk civil liability. Compliance efforts will be essential moving forward.

ISPs should take into consideration a few key points:

- Reviewing reporting mechanisms: If in the past ISPs could only be held liable for damages arising from third-party content after failing to comply with a specific court order mandating its removal (*judicial-takedown*), now the main liability regime establishes that ISPs can be held liable for failing to remove content upon a mere notification. User reports now carry a more relevant weight, and ISPs should review its reporting mechanisms to avoid flaws in receiving and handling user reports;
- Training content moderation teams into new standards: The STF ruling has created several different liability regimes, varying according to each type of content. This

disposition places ISPs in the challenging position of having to assess whether reported content constitutes a crime (and which type of crime) or an illicit act under Brazilian law. Such a responsibility demands not only legal knowledge and interpretation but also swift and accurate decision-making.

Three different categories of crimes – crimes and illicit conducts in general; crimes against honor; and serious crimes (an exhaustive list provided in the Thesis) – require different moderation efforts. To mitigate the risks of potential misjudgments and consequent civil liability, response teams must not only understand the new framework, but also be trained on how to identify each type of content in order to take the applicable moderation measure. It is also advisable to have the support of Portuguese-speaking professionals handling user notices to ensure proper adherence.

- Reported content/accounts that portray crimes or illicit acts must be taken down upon a mere notification, under penalty of the ISP being deemed liable for the damages caused by them (*notice-and-takedown*).
- Content involving crimes against honor continue to fall under the scope of Article 19 (*judicial-takedown*).
- Replicated content involving crimes against honor that has already been deemed as infringing by a court order fall under the *notice-and-takedown* regime. That is, ISPs are required to take it down upon a mere notification.

- **Need to intensify proactive moderation.** ISPs now have a duty of care to prevent the dissemination of content involving serious crimes, and failure to do so shall be deemed a systemic flaw. Also, ISPs are now presumptively liable for illicit content involving serious crimes (in the event of systemic flaw) or in cases involving *(a)* paid advertisement and promoted content; *(b)* artificial distribution networks (chatbots or bots).

  ISPs must intensify proactive moderation of such content, as they shall only be exempt from liability if they can demonstrate that they acted diligently and within a reasonable timeframe to make the content unavailable.

- **New litigation fronts.** The user responsible for content removed due to its association with a serious crime may seek its reinstatement in court. While lawsuits requesting content removal may decline, platforms should anticipate a rise in legal claims challenging content moderation decisions.

- **Accountability efforts.** ISPs must adopt measures aimed at strengthening their responsibility and accountability, such as the developoment of self-regulatory frameworks that necessarily include notification systems, due process mechanisms, and annual transparency reports regarding extrajudicial notices, advertisements, and

promoted content. A DSA-style transparency report should suffice.

- Need for local presence in Brazil. Foreign ISPs operating in Brazil must now constitute a Brazilian subsidirary or contract with a licensed local representative with full full powers to *(a)* respond before administrative and judicial spheres; *(b)* provide competent authorities with information regarding the provider's operation, the rules and procedures used for content moderation and management of complaints through internal systems; transparency reports, monitoring, and management of systemic risks; rules for user profiling (when applicable), advertising, and paid content promoting; *(c)* comply with judicial orders; and *(d)* respond to and comply with any penalties, fines, and financial impacts incurred by the represented entity, especially for non-compliance with legal and judicial obligations.

* * *

04 APPENDIX – COMMENTS TO EACH DISPOSITION OF THE THESIS2

1 Article 19 of Law No. 12,965/2014 (Brazilian Internet Act or MCI), which requires a specific court order for the civil liability of internet service providers for damages arising from content generated by third parties, is partially unconstitutional. There is a state of partial omission that arises from the fact that the general rule of Article 19 does not confer sufficient protection to constitutional legal assets of high relevance (protection of fundamental rights and democracy).

Interpretation of Article 19 of the MCI

2 As long as no new legislation is enacted, Article 19 of the MCI must be interpreted in such a way that internet service providers are subject to civil liability, except for the application of the specific provisions of the electoral legislation and the normative acts issued by the Supreme Electoral Court ("TSE").

Comment: STF's interpretation of Article 19 is provisional and will remain in effect until new legislation is enacted by Congress. However, any future legal framework is expected to align with the core principles established by STF's ruling. Also, prior to each election cycle (each 2 years), the TSE enacts new rules governing the upcoming elections. In 2024, the TSE enacted rules for content moderation during the electoral period. As an example, it determined that platforms can be held jointly liable if they do not proceed with the immediate takedown of content and accounts in what TSE classifies as "risky cases", such as cases related to the spreading of misinformation about candidates. The declaration of partial unconstitutionality of Article 19 does not impact this set of provisions directly related to elections and upcoming ones in the same sense.

3 The internet service provider will be held civilly liable, under the terms of Article 21 of the MCI, for damages arising from content generated by third parties in cases of crime or unlawful acts, without prejudice to the duty to takedown the content. The same rule applies in cases of accounts reported as inauthentic.

Comment: Article 21 establishes a *notice-and-takedown* regime, especifically for non-consensual sharing of intimate content, commonly referred to as revenge porn. However, the *notice-and-takedown* approach is now the rule for any content that portrays crimes, unlawful acts and inauthentic accounts. Also, and more importantly,

[2] This text presents in this Appendix is an unofficial translation of the thesis brought by the Supreme Court.

this disposition places ISPs in the challenging position of having to assess whether reported content constitutes a crime or an illicit act under Brazilian law. Such a responsibility demands not only legal knowledge and interpretation but also swift and accurate decision-making, which may exceed the technical and legal capabilities typically expected from platforms. To mitigate the risks of potential misjudgments, notification response teams should be properly trained to identify possible crimes and illicit acts under Brazilian legislation.

3.1 Article 19 of the MCI applies in the event of a crime against personal honor, without prejudice to the possibility of removal by extrajudicial notification.

Comment: crimes against personal honor comprise the crimes of false accusation, defamation and offensive remarks. Given the inherent subjectivity in the characterization of these crimes, which could hinder the analysis of a notice by the platform, the Supreme Court held that this determination should rest with the Judiciary. Accordingly, ISPs are required to remove infringing content of this nature only upon receipt of a court order, following the original wording of Article 19.

3.2 In the case of successive replications of the offensive fact already recognized by court decision, all social media providers must remove publications with identical content, regardless of new court decisions, based on judicial or extrajudicial notification.

Comment: In summary, replicated content involving crimes against honor that has already been deemed as infringing by a court order fall under the *notice-and-takedown* regime. That is, ISPs are required to take it down upon a mere notification.

Presumption of liability

4 The presumption of liability of providers in case of illegal content is established when it comes to *(a)* paid advertisements and promoted content; or *(b)* artificial distribution network (chatbot or robots). In these cases, the liability may occur regardless of notification. Providers will be excluded from liability if they prove that they have acted diligently and within a reasonable time to make the content unavailable.

Comment: it is advisable that ISPs closely monitor the use of mechanisms *(a)* and *(b)*

as to review the content being promoted and its lawfulness based on the Brazilian legislation. For this task, it is advisable to have the 10upport of Portuguese-speaking professionals or professionals familiar with the Brazilian legislation supervising and moderating promoted content proactively.

Duty of care in case of mass circulation of serious illegal content

5 The internet service provider is liable when it does not promote the immediate takedown of content that constitutes the practices of serious crimes provided for in the following exhaustive list: (a) anti-democratic conducts and acts set forth in Articles 296, sole paragraph, 359-L, 359-M, 359-N, 359-P and 359-R of the Criminal Code; (b) crimes of terrorism or preparatory to terrorism, set forth in Law No. 13,260/2016; (c) crimes of inducement, instigation or assistance to suicide or self-half, under the terms of Article 122 of the Criminal Code; (d) incitement to discrimination on the basis of race, color, ethnicity, religion, national origin, sexuality or gender identity (homophobic and transphobic conduct), set forth in Articles 20, 20-A, 20-B and 20-C of Law No. 7,716/1989; (e) crimes committed against women due to their female gender, including content that propagates hatred or aversion to women (Law No. 11,340/06; Law No. 10,446/02; Law No. 14,192/21; Art. 141, § 3; Art. 146-A; Art. 147, § 1; Art. 147-A; and Article 147-B of the Criminal Code); (f) sexual crimes against vulnerable persons, child pornography and serious crimes against children and adolescents, under the terms of Articles 217-A, 218, 218-A, 218-B, 218-C, of the Criminal Code and Articles. 240, 241-A, 241-C, 241-D of the Statute of the Child and Adolescent; g) human trafficking (Art. 149-A of the Criminal Code).

Comment: ISPs must implement or improve their mechanisms to proactively monitor content related to these specific matters. It is worth noting that some of these crimes – such as racism, religious intolerance and national origin – may be defined an interpreted differently accros jurisdictions. For this reason, it is advisable that the content review teams are familiar with Brazilian Portuguese languagem and/or Brazilian cultural and legal context.

5.1 The liability of internet service providers outlined in this item pertains to the occurrence of a systemic flaw.

5.2 A systemic flaw, attributable to the internet service provider, is considered to occur when the provider fails to adopt adequate measures for the prevention or removal of the previously listed illicit content, thereby constituting a violation

of the duty to act responsibly, transparently, and cautiously.

Comment: Systemic flaws are likely to become identifiable only after the STF's regulatory framework has been in effect for some time, as such failures tend to surface only through continuous deficiencies in moderation and responsiveness to notices and court orders. While litigation based on this rule may be unlikely in the short term, it is essential that platforms strictly comply with the standards set forth in item 5, especially considering that the nature of the content involved (serious crimes) tends to attract public attention on its own. One effective way to demonstrate compliance is by publicly disclosing mitigation efforts, such as through periodic transparency reports.

5.3 Measures are considered adequate if, according to the state of the art, they provide the highest levels of security for the type of activity performed by the provider.

Comment: Although the provision outlines what may qualify as "adequate measures," the definition remains broad and subjective. As such, its practical application will likely depend on case-by-case assessments by the supervising authority, which could undermine legal certainty.

5.4 The existence of illicit content in an isolated, atomized manner is not, by itself, sufficient to trigger the application of civil liability under this item. However, in this case, the liability regime provided for in Article 21 of the MCI will apply.

Comment: This provision indicates that liability for systemic flaws will only arise when ISPs continuosuly fail to diligently remove content involving serious crimes, thereby breaching their duty of care. As such, enforcement of this provision appears to target broader, collective patterns of misconduct and will probably be carried out through collective mechanisms, such as regulatory investigations or class actions, rather than through isolated claims. In individual cases, the applicable framework is the *notice-and-takedown* regime established by Article 21.

5.5 In the cases provided for in this item, the person responsible for publishing the content removed by the internet service provider may request its reinstatement in court, upon demonstration of the absence of illegality. Even if the content is restored by a court order, there will be no imposition of indemnification on the provider.

Comment: ISPs will not face civil liability for removing content related to serious crimes, even if the takedown is later reversed by a court. In contrast, failing to remove unlawful content of this nature may lead to civil liability. As a result, the rule creates a strong incentive for ISPs to err on the side of removal, even in cases of doubt, since mistaken takedowns carry no legal or financial consequences. While this may be justifiable from a risk-management standpoint, it also raises concerns about potential chilling effects on freedom of expression.

Application of article 19

6 Article 19 of the MCI applies to *(a)* e-mail service provider; *(b)* service provider whose primary purpose is to conduct closed meetings by video or voice; *(c)* provider of instant messaging services (also called providers of private messaging services), exclusively with regard to interpersonal communications, protected by the confidentiality of communications (Article 5, item XII, of the Constitution).

Marketplaces

7 Internet service providers that function as marketplaces are civilly liable in accordance with the Consumer Protection Code (Law No. 8,078/90 – "CDC").

Comment: As a general rule, the CDC holds suppliers of products and services strictly liable for damages suffered by consumers. However, exceptions apply, and their applicability depends on the specific circumstances of each case. The Thesis does not address the fact that some ISPs may encompass multiple functions – including marketplace features that enable in-platform purchases – within a single platform. This overlap raises questions as to which civil liability regime should apply. A reasonable approach would be to clearly distinguish between each type of service offered, so that distinct liability regimes can be appropriately assigned to each component.

Additional duties

8 Internet service providers must issue self-regulation that necessarily covers a notification system, due process and annual transparency reports regarding

extrajudicial notifications, ads and boosts.

Comment: The Thesis does not provide any detail on how this notification system should be handled or how due process would take place (*Would this due process encompass a right to appeal platform decisions? Or would it mandate that users should have the right to defend content deemed infringent before it is taken down?*). ISPs should follow carefully the discussions involving this new requirement to assess the necessity of reviewing their practices.

9 They shall also make available to users and non-users specific service channels, preferably electronic, which are accessible and widely disseminated on the respective platforms on a permanent basis.

10 Such rules must be published and reviewed periodically, in a transparent and accessible manner to the public.

11 Internet service providers operating in Brazil must establish and maintain a local presence and a representative in the country, whose identification and contact information must be made available and easily accessible on their respective websites. This representation must grant the representative, necessarily a legal entity headquartered in the country, full powers to (a) respond before administrative and judicial spheres; (b) provide competent authorities with information regarding the provider's operation, the rules and procedures used for content moderation and management of complaints through internal systems; transparency reports, monitoring, and management of systemic risks; rules for user profiling (when applicable), advertising, and paid content promoting; (c) comply with judicial orders; and (d) respond to and comply with any penalties, fines, and financial impacts incurred by the represented entity, especially for non-compliance with legal and judicial obligations.

Comment: The safest form of compliance with this set of rule is by *(i)* adpating the platforms' terms of service and other pages of easy access to users as to provide information about the notification system and the process adopted in portuguese; *(ii)* creating/enhancing transparency reports as to prove compliance with the applicable rules; and *(iii)* setting up a Brazilian subsidirary or a contract with a licensed local representative with full power of attorney.

Nature of liability

12 There shall be no strict liability in the application of the thesis stated herein.

Appeal to the legislator

13 The National Congress is called upon to draft legislation capable of remedying the deficiencies of the current regime in terms of the protection of fundamental rights.

Comment: Several bills proposing new internet regulations are currently pending before Congress. As noted, any future legal framework is expected to align with the core principles established in the Supreme Federal Court's ruling.

Modulation of temporal effects

14 To preserve legal certainty, the effects of this decision are modulated, which will only apply prospectively, except for final and unappealable decisions.

* * *

Rio de Janeiro • Sao Paulo • Brasilia • Curitiba • Tokyo
Lickslegal.com | Copyright © 2026 Licks Advogados
info@lickslegal.com