Civil liability of internet application providers:

the new regime after STF Theme 987 and Decree No. 12,975/2026

AUTHORS

Andressa Bizutti
Partner, Media, Entertainment & Advertising — b/luz

Ana Paula Silveira
Senior Associate, Media, Entertainment & Advertising — b/luz

TRANSLATOR

Vitoria Maciel
Associate, Media, Entertainment & Advertising — b/luz

baptistaluz.com.br

contato@baptistaluz.com.br

Table of Contents

Introduction

The Brazilian Federal Supreme Court (STF) concluded the judgment of General Repercussion Theme 987 (*RE 1.037.396/SP*, Reporting Justice Dias Toffoli), on the constitutionality and interpretation of article 19 of the Brazilian Civil Rights Framework for the Internet (Statute No. 12,965/2014, “MCI”). Upon conclusion of the judgment, the Court confirmed the **partial and progressive unconstitutionality** of article 19 and established its **immediate final and binding effect (res judicata)** on June 17, 2026.

This material organizes the new regime **by subject**. Each row of the table in item 3 below explains the rule on the subject, shows what the STF decided alongside what Decree No. 12,975/2026 (“Decree”) regulated, and indicates the corresponding legal basis.

1. Two instruments, one subject

The liability of application providers for third-party content, as well as their duties, is now governed by two instruments read together: the **STF thesis** and **Decree No. 12,975/2026**, which amended Decree No. 8,771/2016 and regulated the MCI based on the Court’s parameters. The Decree was issued on May 20, 2026, published in the Official Gazette (DOU) of May 21, 2026, and enters into force on July 20, 2026.

2. Thesis × Decree: distinct natures

Although they address the same subject, the two instruments have different natures, and this changes what is required of the provider.

The **thesis** is **interpretation**: it states how article 19 of the MCI must be read until new legislation is enacted, and sets the **civil liability** regime, to be applied by the Judiciary in the specific case.

The **Decree** is **regulation**: it creates rules of conduct whose breach subjects the provider to **administrative sanctions** (art. 12 of the MCI: warning, fine, suspension and prohibition), enforced by the ANPD.

Therefore, the Decree **requires structural compliance** (i.e., permanent governance, processes and documentation), and not merely a reaction to a specific dispute.

	STF Thesis (Theme 987)	Decree No. 12,975/2026
Nature	Constitutional interpretation of article 19 of the MCI (how the law must be read).	Infra-legal regulation: rule of conduct that regulates the MCI.
What it establishes	The civil liability regime of providers, until new legislation is enacted.	Duties, procedures and standards for organization, moderation and risk management.
How it applies	Applied by the Judiciary, in the specific case (as a rule, reactively).	Enforced by the ANPD (art. 19-A), continuously and preventively (*ex ante*).
Breach	Civil liability (duty to indemnify).	Administrative sanctions (art. 12 of the MCI): warning, fine, suspension and prohibition.
Requires from the provider	Diligent conduct, assessable case by case.	Structural and permanent compliance: governance, processes and documentation.

In practice: the thesis defines when there is a duty to indemnify; the Decree defines how the provider must organize itself in order not to be sanctioned.

3. Thematic table: the regime subject by subject

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
1. Why the regime changed	Article 19 of the MCI required breach of a specific court order to hold the provider liable for third-party content. The STF declared this article partially unconstitutional, for not sufficiently protecting fundamental rights and democracy. Until new legislation is enacted, article 19 is now interpreted such that application providers are subject to civil liability, except as provided in electoral legislation and TSE rules.	Issued by the Executive, the Decree regulates the MCI and creates a dedicated chapter on the liability of application providers, detailing duties of conduct, procedures and enforcement.	**Thesis:** items 1 and 2 **Decree:** art. 1 and Chapter III-A
2. General rule: third-party	The application provider is civilly liable, jointly and severally with the author, for damages caused by third-party content	Upon receiving a notice, the provider must take down third-party content that constitutes a crime, except crimes against honor.	**Thesis:** items 3 and 3.1

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
content (crime or unlawful act)	that is a crime or unlawful act, and has the duty to remove it. It is not liable if it demonstrates that there was reasonable doubt as to the unlawfulness, after a qualified diligence analysis. The same joint-and-several rule applies to accounts reported as inauthentic.	It may keep it online if, after a diligent and reasoned analysis, it concludes that there is reasonable doubt as to the criminal nature - weighing the doubt against the seriousness of the crime - and, in that case, must explain to the notifier why it kept the content. In enforcement, the assessment looks at whether the provider acted diligently, proportionately and swiftly; it cannot be punished merely for having kept or removed an isolated piece of content. Lastly, in applying the article, the provider must consider the context of the posts, religious freedom and freedom of belief, and any informational, educational, critical, satirical or parodic purpose.	**Decree:** arts. 16-G (caput, §1 and §2) and 16-I
3. Crimes against honor	For a crime or civil wrong against honor (slander, insult, defamation and the like), the former rule of article 19 continues to apply: the provider is liable only if it fails to comply with a court removal order. Even so, voluntary removal upon extrajudicial notice is possible.	Confirms that, for crimes and unlawful acts against honor, the provider's liability depends on a specific court order.	**Thesis:** item 3.2 **Decree:** art. 16-J, item I
4. Replication of an offensive fact already recognized in court	Where a court decision has already recognized that certain content is offensive and it is published again (identical copies), all social-media providers must remove it without a new decision, judicial or extrajudicial notice being sufficient.	Applies the same rule and broadens it: it covers all application providers that intermediate third-party content.	**Thesis:** item 3.3 **Decree:** art. 16-J, sole paragraph
5. Duty of care and systemic failure (serious crimes)	For a closed list of serious crimes, the provider is liable if it does not remove the content immediately. They are: (a) anti-democratic acts; (b) terrorism and preparatory acts of terrorism; (c) inducement, instigation or assistance to suicide or self-mutilation; (d) incitement to discrimination based on race, color, ethnicity, religion, national origin, sexuality or gender identity (homophobia and transphobia); (e) crimes against women on account of the female sex, including hatred of women; (f) sexual crimes against vulnerable persons, child pornography and serious crimes against children and adolescents; (g) human trafficking. This liability is for "systemic failure": failing to adopt adequate prevention or removal measures, in accordance with	Repeats the same list of crimes (in a different order: I terrorism; II suicide/self-mutilation; III discrimination; IV crimes against women; V sexual crimes against vulnerable persons and exploitation of children and adolescents; VI human trafficking; VII anti-democratic acts). It provides that the provider commits systemic failure when it fails to demonstrate that it adopted adequate measures that, in accordance with the state of the art, (i) provide the highest levels of security and (ii) curb the massive circulation of such content. The authority assesses the failure through supervision and periodic	**Thesis:** items 5 and 5.1 to 5.6 **Decree:** arts. 16-B (items I–VII and §§ 1–5) and 16-C

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
	the state of the art, with the highest levels of security. An isolated piece of content is not enough to constitute systemic failure; in that case the general rule applies (liability arises only after notice). Anyone whose content was removed may ask the courts to reinstate it, proving it was not unlawful; and, even if it is reinstated, the provider pays no damages. Provisional relief may also be sought to prevent removal.	analysis, not case by case; isolated content does not characterize it. The provider must supply the authorities with the data evidencing the measures; as to crimes against children and adolescents, Statute No. 15,211/2025 (Digital ECA) also applies. It must also diligently monitor, identify, assess and manage the systemic risks created or heightened by its activities or by the circulation of content involving serious crimes.	
6. Advertising, paid boosting and inorganic dissemination	The provider's fault is presumed (a rebuttable presumption, admitting evidence to the contrary) when the unlawful content appears in (a) paid advertising and boosting or (b) artificial mechanisms of inorganic dissemination. In these situations it may be held liable regardless of notice. It is released from liability if it proves that it acted diligently and within a reasonable time to take the content down.	The provider's liability is presumed when the unlawful content is run in advertising, paid boosting or distributed through artificial distribution networks, regardless of notice; it is exempt if it demonstrates diligent action within a reasonable time to take it down. It must also adopt measures to prevent the contracting of advertising or boosting of criminal or unlawful content and retain, for one year (counted from the end of the run), the information on each advertisement/boost and its advertisers.	**Thesis:** item 4 **Decree:** arts. 16-L, 16-K, 16-M and 16-A, III
7. Misleading, abusive or fraudulent advertising	There is no specific item. Consumer protection appears in the subjection of marketplaces to the CDC (next subject).	Upon receiving notice, the provider must take down third-party content that is misleading, abusive or fraudulent advertising (art. 37 of the CDC). The notice may come from a body of the National Consumer Protection System or, where public policy is involved, from the AGU. Any advertising that the user cannot clearly identify as such is deemed misleading.	**Thesis:** — **Decree:** art. 16-N (caput, §§ 1 and 2)
8. Marketplaces (consumer relationship)	Providers that operate as marketplaces are civilly liable under the Consumer Protection Code (Statute No. 8,078/90).	Does not directly address the liability of marketplaces; it deals with the consumer relationship only in the advertising part (previous subject). The extent of liability in the consumer chain will depend on the specific case, based on the CDC.	**Thesis:** item 6 **Decree:** no specific provision
9. Notice and due process	No specific provision.	The notice must contain, under penalty of nullity: (i) elements identifying the possible criminal or unlawful conduct (or the court	**Thesis:** items 7 and 9 **Decree:** arts. 16-D, 16-E and 16-F

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
		decision, in the case of replication); (ii) information allowing the specific content to be located; and (iii) identification of the notifier and, where applicable, the basis of its standing. Upon receiving the notice, the provider confirms receipt and decides in a reasoned manner: if it removes, it notifies the notifier and the author of the content, with the reason and how to challenge it; if it keeps it, it notifies the notifier, with the reason and how to challenge it; if it reconsiders after a challenge, it informs both. It must adopt measures to curb the abusive use of notices, especially against freedom of expression. The authority may regulate the form, deadlines, eligible notifiers, challenges and other necessary procedures.	
10. Reporting crimes to the authorities	No specific provision.	Upon identifying content relating to the criminal conducts, the provider must forward to the Government the content and the information necessary to identify authorship and materiality. The form will be governed by an act of the Minister of Justice and Public Security, including the possibility of sending it to a central body.	**Thesis:** — **Decree:** art. 16-H
11. Record retention and traceability	No specific provision.	Mandatory retention of IP records now includes the associated source logical port, whenever necessary to reliably identify the originating terminal or the next network link. This duty does not depend on a prior request and falls on each provider; the provision of such data follows the access rules already set out in the MCI.	**Thesis:** — **Decree:** art. 15-A (caput and §§ 1 and 2)
12. Self-regulation and transparency	Providers must issue self-regulation that mandatorily includes a notice system, due process and annual transparency reports on extrajudicial notices, advertising and boosting. These rules must be published and periodically reviewed, transparently and accessibly to the public.	Repeats these obligations (terms of use and self-regulation with a notice system, due process and annual transparency reports), with periodic publication and review. Self-regulation will be considered evidence of good faith in the investigation of infractions, where aimed at creating technical and governance standards that protect users' rights. The provider must	**Thesis:** items 7 and 9 **Decree:** arts. 20-A and 16-A, IV-B

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
		also adopt means to ensure the security and transparency of the services.	
13. Service and reporting channels	Providers must offer users and non-users specific service channels, preferably electronic, accessible, widely publicized and permanent.	They must maintain a permanent and easily accessible reporting channel to receive and handle notices, expressly including the reporting of criminal or unlawful content.	**Thesis:** item 8 **Decree:** art. 16-A, item II
14. Local seat and representative	Providers operating in Brazil must maintain a seat and a representative in the country (a legal entity), with identification accessible on their websites. The representative must have full powers to: (a) respond in administrative and judicial proceedings; (b) provide the authorities with information on the provider's operation, the moderation and complaint-management rules, the transparency and systemic-risk-management reports, and the rules on profiling, advertising and paid boosting of content; (c) comply with court orders; and (d) be liable for penalties, fines and financial impacts.	Establishes the same requirement of a local seat and legal representative, with equivalent powers (subparagraphs "a" to "d", including the information-provision details). The representative is a legal entity and its contact information must be easily accessible on the represented party's website.	**Thesis:** item 10 **Decree:** art. 16-A, item I and sole paragraph
15. Services excluded from the new regime	Only article 19 continues to apply (liability only after a court order) to: (a) email, as to interpersonal communications protected by confidentiality; (b) services whose main purpose is a closed video or voice meeting; (c) instant/private messaging, as to interpersonal communications protected by confidentiality; and (d) other providers that do not interfere in the flow of communication and information.	For these services, neither the duty of care nor the duties of notice, takedown and the other obligations of the new regime apply - only the court-order rule continues to apply. They are: (I) email (messages between recipients identifiable by domain); (II) instant messaging, in confidential interpersonal communications, without public dissemination or open groups; and (III) audiovisual communication in a restricted group (meetings and calls among invited participants, in a controlled environment).	**Thesis:** item 3.4 **Decree:** art. 16-O (items I–III) and art. 16-J, II
16. Limits of liability	There is no strict liability: the provider is not automatically liable; an analysis of its conduct is always required.	The provider cannot be held liable merely for having kept or removed an isolated piece of content; and the authority is prohibited from notifying the provider to moderate isolated content (enforcement is systemic, not case by case).	**Thesis:** item 11 **Decree:** art. 16-I (caput and sole paragraph)
17. Differentiated criteria by size	No specific provision.	The authority may set differentiated criteria for compliance with the duties according to the provider's	**Thesis:** — **Decree:** art. 16-P

Subject	What the STF decided (Thesis — Theme 987)	How the Decree regulated it	Legal basis
		economic size, the level of interference in the circulation of content, the state of the art and the risk of the service - with special attention to small providers.	
18. Enforcement and sanctions (ANPD)	The thesis recognizes the Executive's authority to regulate, supervise and investigate providers' obligations, and calls on Congress for a law on the subject.	The ANPD is the authority responsible for regulating, supervising and investigating infractions regarding providers' duties, in light of the MCI, the LGPD and Statute No. 15,211/2025. Infractions are investigated by the ANPD and the applicable sanctions are those set out in art. 12 of the MCI: warning, fine, suspension and prohibition of activities.	**Thesis:** item 12 **Decree:** art. 19-A
19. Entry into force and effects over time	The decision applies prospectively (*ex nunc* effects), as from publication of the merits trial-session minutes (August 5, 2025), preserving acts already performed; continued or permanent acts are excluded from this limitation, and decisions already final and binding are respected. Providers have 60 days, counted from publication of the minutes of the motion for clarification (*embargos de declaração*), to implement the duty-of-care obligations (serious crimes).	Enters into force 60 days after publication. Published in the DOU on May 21, 2026, it takes effect on July 20, 2026.	**Thesis:** items 13 and 14 **Decree:** art. 2

4. Notes to the table

Points of attention and drafting differences between the two instruments:

Point	Observation
Presumption of fault × of liability	The thesis speaks of a "(rebuttable) presumption of fault"; the Decree says "liability is presumed". The difference must be read in light of "there is no strict liability" (thesis, item 11) and of art. 16-I.
Same list of crimes, different order	The list of serious crimes is identical in the thesis (item 5, "a" to "g") and in the Decree (art. 16-B, I to VII); only the order changes. As to crimes against children and adolescents, the Decree adds the application of Statute No. 15,211/2025 (Digital ECA). Thus, if the systemic failure involves sexual crimes against vulnerable persons, sexual exploitation of children and adolescents and serious crimes against children and adolescents, liability may be joint and several (art. 15 of Statute No. 15,211, of September 17, 2025).
Replication: broadened scope	The thesis limits the replication rule to social media (item 3.3); the Decree extends it to all providers that intermediate third-party content (art. 16-J, sole paragraph).
Marketplaces	Subjection to the CDC comes from the thesis, not from the Decree, which deals only with unlawful advertising. The extent of liability in the consumer chain will depend on the specific case.

5. Open points

- The delimitation of "duty of care", "systemic failure", "systemic risks" and "state of the art", and the authority's criteria for assessing the sufficiency of measures.
- The scope of "reasonable doubt" and the standard of "qualified diligence" required before keeping content online.
- The temporal coexistence: the thesis already produces effects, while the Decree only takes effect as from July 20, 2026.
- The pending ANPD regulation (deadlines, parties with standing to notify, the form of access to data and criteria by size).
- The drafting difference between the thesis and the Decree on advertising and boosting and its impact on the burden of proof.
- The progress, in Congress, of legislative bills seeking to suspend the Decree.
- The operationalization of the "periodic analysis" provided for in § 2 of art. 16-B of the Decree (i.e., frequency and how this analysis will be conducted).

6. Insights

The regime moves closer to continuous risk-assessment models. The reference to the state of the art and to systemic-risk management shifts the focus from one-off removal to the adequacy of structures, making documented governance and audit trails central to the provider's defense.

The defense shifts to proof of diligent and timely action. In advertising and boosting, the presumption shifts the burden to the provider, placing value on prior verification and on recording the measures taken.

The concrete risk of each operation results from reading the thesis and the Decree together, calibrated by size and by type of service. It is in this calibration that what each provider must, in practice, demonstrate is defined.

7. Closing

The picture will still consolidate with the ANPD's regulation, case-law application and the possible action of Congress. Until then, the thesis and the Decree form a single regime, to be applied in an integrated manner. Reviewing the moderation policies, notice flows and governance structures in light of these parameters is the recommended step to reduce exposure.

b/luz

www.baptistaluz.com.br

/company/baptistaluzadvogados

baptistaluzadvogados/

@baptistaluzadvogados

São Paulo

Rua Ramos Batista, 444 / 3º andar
Vila Olímpia / São Paulo / SP
CEP 04552-020 / Brasil

Londrina

Av. Ayrton Senna da Silva, 300 / Sala 1801
Gleba Palhano / Londrina / PR
CEP 86050-460 / Brasil

Florianópolis

Rodovia José Carlos Daux, 4100
Primavera Office / 3ª Andar
Saco Grande / Florianópolis / SC
CEP 88032-005 / Brasil