

Platform liability

Revision of Article 19 of the Brazilian Internet Civil Rights Framework (Marco Civil da Internet)

What changes in practice with the Federal Supreme Court's new ruling
and the government's decrees?

SUMMARY

1. What was at stake?

2. Key legislation

1. Federal Supreme Court (STF)
2. Decress

3. Who are the application providers?

4. What was the rule?

5. What were the exceptions?

6. What changes with the Federal Supreme Court's decision and the decrees?

1. Art. 21 becomes the rule
2. Art. 19 still prevails
3. Relative presumption of fault
4. Identical content
5. Duty of care for serious tortious acts (systemic failure)
6. Marketplaces
7. Self-regulation
8. Representation in Brazil
9. Subjective liability
10. Regulation of the issue by the Executive Branch and not solely by Congress
11. Temporal effects of the Federal Supreme Court's decision

7. Decree No. 12,975/2026 - Updates the MCI regulations

1. Obligation to report crimes to the authorities
2. Duty to retain IP address records
3. ANPD

8. Decree No. 12,976/2026 - Protection of women on the internet

Authors

About Us

VK ADV



1. What was at stake?

A responsabilidade civil dos provedores de aplicação de internet por danos The civil liability of internet service providers for damages resulting from content generated by third parties.

In a case concluded on June 17, 2026, the Federal Supreme Court (STF) ruled on the arguments regarding the partial and progressive unconstitutionality of Article 19 of the Internet Civil Rights Framework (MCI). In May, the government issued decrees regulating the matter.

2. Key Legislation

1. STF

- In a ruling dated June 26, 25, the STF had recognized the partial and progressive unconstitutionality of Article 19 of the MCI. [Read here the summary](#) of Extraordinary Appeals RE 1,037,396 (Issue 987) and RE 1,057,258 (Issue 533).
- After the platforms filed motions for clarification, the legal principle established regarding the MCI was refined in the conclusion of the ruling, which was finalized on June 17, 26. [Read the final text of the legal principle here.](#)

2. Decrees

- On May 21, 2026, Decrees No. 12,975/2026 ([here](#)) and No. 12,976/2026 ([here](#)) were published to regulate the matter, among other things, granting the National Data Protection Agency (ANPD) the authority to regulate, oversee, and investigate related violations.

3. Who are the application providers?

Companies that provide services via the Internet, such as social media platforms, e-commerce sites, marketplaces, and email service providers.

The decrees and the STF ruling emphasize that the new obligations focus on providers that act as intermediaries for third-party generated content, with exceptions maintained for services such as email, private messaging, and videoconferencing in restricted environments.

4. What was the rule?

Civil liability of applications applies **only in the event of failure complying with a court order**:

Art. 19. To ensure freedom of expression and prevent censorship, an internet service provider may only be held civilly liable for damages arising from third-party generated content if, following a specific court order, it fails to take steps to make the content identified as infringing unavailable.

This did not prevent providers from moderating their users' content out of court.



5. What were the exceptions?

Civil liability **arising from failure to comply with extrajudicial notice**, but only for unauthorized pornography and copyright infringement:

*Art. 21. An internet application provider that makes third-party generated content available shall be held jointly and severally liable for **invasion of privacy resulting from the unauthorized disclosure of images, videos, or other materials containing scenes of nudity or private sexual acts by its users** when, after receiving a notice, it fails to take steps to make such content unavailable.*

*Art. 31. Until the specific law provided for in § 2 of Art. 19 enters into force, the liability of internet application providers for damages arising from third-party generated content, **in cases involving infringement of copyright or related rights**, shall continue to be governed by the copyright legislation in force on the date this Law enters into force.*

6. What changes with the Federal Supreme Court's decision and the decrees?

1. Art. 21 Becomes the rule

Joint and several civil liability arising from failure to comply with extrajudicial notice, for:

a) Crimes or unlawful acts, in general, without prejudice to the duty to remove the content, unless the provider demonstrates reasonable doubt as to the unlawfulness after conducting a due diligence review. This creates a significant layer of governance: the platform must demonstrate the process, criteria, and evidence of its review to avoid liability; and

b) Accounts reported it as inauthentic.



2. Art. 19 still applies

Civil liability applies only in the event of failure to comply with a court order, for:

- a) **Crimes against honor**, without prejudice to the possibility of removal upon extrajudicial notification;
- b) **Email service providers**, exclusively with respect to interpersonal communications, protected by the confidentiality of communications;
- c) Application providers whose primary purpose is to **facilitate closed video or voice meetings**;
- d) **Instant messaging service** providers (also known as private messaging service providers), exclusively with respect to interpersonal communications, which are protected by the confidentiality of communication; and
- e) Other internet application providers do not interfere with the flow of communication and information.

3. Relative presumption of fault

- a) **Paid advertisements and promotions**; or
- b) **Artificial mechanisms for the inorganic dissemination of unlawful content**.

In these cases, liability may apply regardless of notification, unless the providers can prove that they acted diligently and within a reasonable time to make the content unavailable.

Decree No. 12,975/2026 also reinforces operational obligations in this regard: maintaining records of ads and advertisers for one year after the campaign ends.





4. Identical content:

Successive replications of the offensive content already recognized by a court decision (with identical content) must be removed regardless of new court decisions, upon judicial or extrajudicial notification to all social media providers.

Decree No. 12,975/2026 reinforces this principle for all providers that act as intermediaries for third-party generated content, establishing a practical obligation to respond to identical content already judicially recognized as offensive.

5. Duty of care for serious criminal offenses (systemic failure)

Liability arises when a provider fails to immediately remove content that constitutes serious criminal acts, as specified in the following exhaustive list:

- (a) anti-democratic conduct and acts;
- (b) crimes of terrorism or acts preparatory to terrorism;
- (c) crimes of inducing, instigating, or aiding suicide or self-harm;
- (d) incitement to discrimination based on race, color, ethnicity, religion, national origin, sexual orientation, or gender identity;
- (e) crimes committed against women;
- (f) sexual crimes against vulnerable persons, child pornography, and serious crimes against children and adolescents; and
- (g) human trafficking.

What is systemic failure?

When the provider **fails to adopt adequate measures to prevent or remove the illegal content listed above, thereby violating its duty to act responsibly, transparently, and prudently.**

For this purpose, **measures** shall be considered **adequate** if, in accordance with the state of the art, they provide the highest levels of security for the type of activity carried out by the provider.

The existence of unlawful content in an isolated, fragmented manner is not, in and of itself, sufficient to trigger civil liability under this provision. However, in such cases, the liability regime set forth in Article 21 of the MCI shall apply.

The party responsible for publishing the removed content may file a lawsuit to have it reinstated, provided they can demonstrate that the content was not unlawful. Even if the content is restored by court order, the service provider will not be required to pay damages.

The provider or the party responsible for publishing the content may also file a petition in court for a preliminary injunction to prevent the removal of the content.

6. Marketplaces

They are civilly liable in accordance with the Consumer Protection Code.

7. Self-regulation

- a) They must establish self-regulatory policies that necessarily include a notification system, due process, and annual transparency reports regarding out-of-court notifications, advertisements, and promoted content; and
- b) They must make specific customer service channels—preferably electronic—available to users and non-users alike, which must be accessible and widely publicized on their respective platforms on a permanent basis.

8. Representation in Brazil

Providers operating in Brazil must establish and maintain a headquarters and a representative in the country, with full authority to comply with the provisions of the STF decision, including responding to and paying any penalties, fines, and financial sanctions incurred by the represented party, especially for failure to comply with legal and judicial obligations.

9. Subjective liability

There will be **no** strict liability in the application of this ruling.

10. Regulation of the matter by the Executive Branch and not solely by Congress

The STF **recognized the Executive Branch's authority to regulate this matter** and to determine the organization, jurisdiction, and operation of the Federal Administration, pursuant to Article 84, VI, a, of the Federal Constitution, **particularly with regard to the functions of regulation, oversight, and enforcement of the obligations imposed on providers of internet applications, as set forth in the decision.** In practice, it upheld the decrees.

Furthermore, the STF called on the National Congress to draft legislation capable of addressing the shortcomings of the current regime regarding the protection of fundamental rights.

11. Temporal effects of the STF's decision

- a) **Effects only for the future:** to preserve legal certainty, the decision will take effect only as of the date of publication of the judgment minutes (August 5, 2025), with only ongoing or permanent acts being exempt from the adjustment; and
- b) **Deadline for implementing structural obligations:** 60 (sixty) days from the publication of the minutes of the ruling on the motion for clarification.





7. Decree No. 12,975/2026 - Updates MCI regulations

Decree No. 12,975/2026 ([here](#)) updates the MCI's 2016 regulations (Decree No. 8,771, [here](#)) to expressly set forth the obligations applicable to internet application providers, including:

- the requirement to maintain a registered office and a legal representative in Brazil;
- the provision of a permanent and accessible channel for reporting illegal content;
- the adoption of measures to prevent the operation of artificial networks for the dissemination of illegal content;
- duties regarding transparency, security, and governance; and
- circumstances under which liability may arise for “systemic failure” in the prevention or removal of certain criminal content.

In addition to the points already discussed in section 6 of this document, the Decree provides for:

1. Obligation to report crimes to the authorities

Platforms must forward criminal content and information necessary to identify the perpetrator and the nature of the offense to the competent authorities, a process that will be further regulated by the Ministry of Justice and Public Security.

2. Obligation to retain IP address records

By internet service providers and internet application providers, including the associated source logical port whenever necessary for the unambiguous identification of the source terminal or the next network link. The obligation to retain the source logical port shall not be contingent upon a prior request and shall rest independently with each provider.

3. ANPD

The ANPD shall play a central role in regulating, supervising, and investigating violations related to the duties imposed on internet application providers, particularly with regard to the protection of users' rights and compliance with the obligations of moderation, transparency, security, and governance set forth in the decree.



8. Decree No. 12,976/2026 - Protection of women on the internet

Decree No. 12,976/2026 ([link](#)) establishes a specific framework for protecting women against digital violence. The text defines various forms of violence against women in the digital environment, such as online harassment, the dissemination of intimate content without consent, political violence, harassment, digital stalking, and the use of AI to create fake intimate images ("deepfakes") and requires providers to adopt preventive measures and ensure the rapid removal of such content.

Among the key points are:

- platforms are also held accountable for "systemic failures" in preventing and removing illegal content targeting women;
- it mandates the provision of specific reporting channels, with reference to the "Ligue 180" hotline;
- it establishes short deadlines for content removal, including up to 2 hours for unauthorized intimate content;
- it requires the automatic blocking of the resending of removed intimate images;
- it mandates measures to reduce the reach of coordinated attacks and harassment campaigns against women, even without the need for a prior complaint; and
- prohibits AI tools from generating or modifying intimate content belonging to third parties.

Decree No. 12,976/2026 also provides for the ANPD's role in enforcement and the creation of an integrated system for the protection and support of victims.



AUTHORS



Rony Vainzof

rony@vlklaw.com.br



Caio Lima

caio@vlklaw.com.br



Tayná Araújo

tayna.araujo@vlklaw.com.br

ABOUT US

At VLK, **law is not a barrier**. It is a catalyst for innovation, enabling business and helping build a more prosperous and equitable society.

We are a boutique law firm specializing in Digital Law, driven by delivering work that makes a difference.

We bring together:

- » Risk and opportunity;
- » Complexity and clarity; and
- » Protection and progress.

No matter how ambitious the project, **we make it happen**, securely, while cutting through unnecessary formalities, across the following areas:

- » Personal Data Protection
- » Ethical and Responsible AI Governance
- » Cybersecurity and Incident Response
- » Legal Marketing and Intellectual Property
- » Technology Regulation
- » Strategic Litigation