Civil Liability of Internet Application Providers

New Developments in the Digital Environment

Authors:

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

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

Fernando Bousso
| Coordinating Partner of the Technology, Data Governance, and Media & Entertainment teams — b/luz

Thiago Xavier Peregrino
| Associate in the Data Governance team — b/luz

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

b/luz

b/luz

Table of Contents

Introduction 3

1. MCI DECREE 3
   - 1.1. General duties of internet application providers 4
   - 1.2. Duty of care and risk management 5
   - 1.3. Notice-and-action system 6
   - 1.4. Disabling access to content and interaction with authorities 6
   - 1.5. Advertising, paid boosting and presumed liability 7
   - 1.6. Scope of application and differentiated criteria 8
   - 1.7. Governance, self-regulation and oversight 8
   - 1.8. Record-Keeping Obligation 9

2. DECREE ON THE PROTECTION OF WOMEN 10
   - 2.1. Duty of care and liability for systemic failure 10
   - 2.2. Notice-and-action system for illegal content 10
   - 2.3. Mitigation of coordinated digital harassment 11
   - 2.4. Prohibition on the generation of intimate content by artificial intelligence 11
   - 2.5. Retention and forwarding of information to public authorities 12

3. DISCUSSION IN CONGRESS 12

Notable provisions include the imposition of duties on internet application providers and the delineation of civil liability regimes.

Introduction

Yesterday, May 21, 2026, two decrees relevant to structuring the operation of the internet in Brazil were published. The first was Decree No. 12,975, of May 20, 2026 ("**MCI Decree**"), which amends Decree No. 8,771/2016, the decree that regulates the Brazilian Internet Bill of Rights ("MCI").

The second was Decree No. 12,976, of May 20, 2026 ("**Decree on the Protection of Women**"), which aims to establish guidelines for the protection of women online. Both decrees take effect sixty days after their publication, on July 21, 2026

1. MCI DECREE

The MCI Decree follows from the decision rendered by the Federal Supreme Court ("STF") in Theme 987 in June 2025, which determined that Article 19 of the MCI must be interpreted in light of the Federal Constitution and established new parameters for holding internet application providers liable for content posted by third parties. Until then, the effective application of the thesis established by the STF ("Thesis") still depended on the decision on the merits becoming final and unappealable, meaning that the obligations described therein remained suspended.

Considering this framework, the Federal Government issued the MCI Decree with the purpose of regulating the MCI based on the parameters defined in the Thesis, replicating points established by the STF while adding specific new duties regarding providers' operations, organization, moderation and risk management, as well as amending rules related to the record-keeping obligation.

Despite the new text, open questions remain, especially regarding the delineation of the duty of care and the criteria for assessing compliance with these obligations.

See below the main developments and impacts.

1.1. General duties of internet application providers

Regarding the general duties of internet application providers, the MCI Decree largely replicates the provisions of the STF decision described in item 11 of the Thesis.

Accordingly, internet application providers must establish and maintain a registered office and a legal representative in Brazil, through a legal entity (Article 16-A, main section and sole paragraph). The legal representative must have authority to (Article 16-A, I):

- respond before administrative and judicial authorities;
- comply with court orders and any applicable sanctions;
- provide the competent authorities with information on:
  - the provider's operations;
  - the rules and procedures used for content moderation and for handling complaints through internal systems;
  - transparency, monitoring and systemic risk management reports; and
  - rules for user profiling, advertising placement and paid boosting of content.

What is new?

The MCI Decree introduces new provisions by establishing that providers must:

i. make available a permanent and easily accessible reporting channel for receiving and handling notices, which expressly includes the possibility of reporting criminal or illegal content (Article 16-A, II);

ii. adopt measures to prevent the operation of artificial distribution networks for illegal content (Article 16-A, III); and

iii. adopt the necessary means to ensure the security and transparency of their services (Article 16-A, IV).

Points to Watch

The MCI Decree does not clearly define the level of action expected from providers to prevent the operation of artificial distribution networks for illegal content or to adopt means to ensure the security and transparency of their services. These matters are likely to be subject to future regulation by the Brazilian National Data Protection Authority ("ANPD"), which was assigned responsible for regulating the matter, as discussed below.

1.2. Duty of care and risk management

The MCI Decree replicates the Thesis by establishing that internet application providers that act as intermediaries for third-party-generated content will be held liable in the event of a systemic failure to immediately disable access to content that constitutes serious crimes, such as terrorism, inducement to suicide, racism, misogyny, among others (Article 16-B).

What is new?

The MCI Decree expressly establishes that:

i. an internet application provider will be deemed to have incurred a systemic failure if it fails to prove the adoption of appropriate measures to prevent or remove the illegal content defined in the main section of Article 16-B, namely measures that (Article 16-B, §1):

   a. provide, in accordance with the state of the art, the highest levels of security for the type of service they offer; and

   b. inhibit the mass circulation of the content referred to in items I to VII of the main section.

ii. the assessment of whether a systemic failure has occurred will be carried out by the competent authority based on supervision mechanisms and periodic analysis (Article 16-B, §2), and providers must make available to the competent authorities the information and data necessary to verify the adoption and application of the measures by the provider; and

iii. the obligation to monitor, identify and manage systemic risks arising from the platform's activities (Article 16-C), bringing the Brazilian regime closer to models based on continuous risk assessment.

Points to Watch

Open questions still remain, especially regarding the delineation of what constitutes "systemic failure," "systemic risks" and "duty of care," as well as the criteria that will be used by the authorities to assess the sufficiency of the measures adopted by providers (Article 16-B, §2). In line with what the STF had already provided for in the Thesis (item 5.4), the isolated existence of such illegal content does not, in and of itself, characterize systemic failure (Article 16-B, §3). These matters will likely be defined by the ANPD in the future.

In addition, the reference to the "state of the art," which was also included by the STF (item 5.3 of the Thesis) and has now been incorporated into the MCI Decree (Article 16-B, §1), indicates that the level of diligence must keep pace with the solutions available in the market. However, the concept remains open-ended and raises questions regarding its proportional application to providers of different sizes, since companies of different sizes will have different budgets to implement detection systems. Therefore, adopting the most advanced technology available may not always be feasible.

1.3. Notice-and-action system

The notice-and-action model for illegal content had already been recognized by the STF (items 8 and 9 of the Thesis) and is now structured in greater detail by the MCI Decree, which establishes minimum requirements for the validity of notices (Article 16-D).

What is new?

The MCI Decree introduces new provisions by establishing:

i. the obligation of providers, once notified, to acknowledge receipt, assess the content and provide the grounds for their decision, whether to remove or maintain the content. In the case of removal, providers must notify both the notifying party and the user responsible for the content; in the case of maintenance, they must notify the notifying party. In both cases, providers must inform the relevant parties of the means available to challenge the decision (Article 16-E);

ii. the minimum requirements for the validity of notices (Article 16-D), such as the need to identify the notifying party and the content to which access is to be disabled; and

iii. the duty of providers to curb the abuse of notice mechanisms (Article 16-F), especially where there is a risk to freedom of expression. However, there are no clear criteria for determining when a notice becomes abusive, which may create uncertainty regarding the limits of such action and the risk of liability for undue restriction of content.

Points to Watch

As a point of attention, the applicable deadlines, persons with standing to submit notices and procedures have not yet been fully defined, and will likely be subject to future regulation (Article 16-D, sole paragraph).

In addition, with respect to Article 16-F, there are no clear criteria for defining what would constitute abuse of notice mechanisms that providers must curb. This may create uncertainty regarding the limits of such action and the risk of providers being held liable for any undue restriction of internet users' right to report content.

1.4. Disabling access to content and interaction with authorities

The MCI Decree maintains the obligation to disable access to criminal content upon notice, **even without a court order**, except in specific cases such as crimes against honor (Articles 16-G and 16-J).

What is new?

MCI Decree provides that:

i. the possibility of maintaining content where there is reasonable doubt as to its unlawful nature, provided that the decision is reasoned and proportionate, taking into account the context of the posts, religious freedom and freedom of belief, and any informative, educational, critical, satirical or parody-related purpose (Article 16-G, §1 and §2);

ii. the obligation to share information with public authorities in cases involving criminal content (Article 16-H), reinforcing the role of providers as active players in the enforcement chain. The Ministry of Justice and Public Security will regulate the manner of compliance with this article; and

iii. the criteria for determining administrative liability, which must take into account the provider's diligent, proportionate and timely action in handling notices, **while prohibiting decisions based exclusively on the isolated removal or maintenance of content** (Article 16-I).

Points to Watch

Questions remain regarding the limits of the obligation to disable access to content, especially with respect to the definition of "reasonable doubt" and the level of depth expected from platforms in their content analysis.

In addition, the obligation to share information with public authorities may create a scenario of hypervigilance in which providers, in order to avoid liability, end up sharing information about internet users who were subject to notices, even without the crime having in fact been proven.

1.5. Advertising, paid boosting and presumed liability

In line with item 4 of the Thesis, the MCI Decree consolidates the presumption of providers' liability when illegal content is disseminated through ads, paid boosting or artificial distribution networks, regardless of notice (Article 16-L). This presumption may be rebutted upon proof of diligent action within a reasonable time (Article 16-L, sole paragraph), which reinforces the importance of robust compliance and advertising moderation structures.

What is new?

The MCI Decree provides for specific obligations applicable to providers that offer ads and boosting tools, which had no express counterpart in the Thesis:

i. the obligation to store information on ads and advertisers for a period of 1 (one) year, counted from the end date of the ad placement, and the competent authority may regulate the manner of access to such information (Article 16-M);

ii. the duty to disable access to misleading, abusive or fraudulent advertising upon notice from competent authorities (Article 16-N); and

iii. content that is not clearly identifiable by users as advertising will be considered misleading advertising (Article 16-N, §2).

Points to Watch

As an open point, there is still uncertainty regarding the parameters for characterizing diligence and "reasonable time."

In addition, content generated by digital influencers that does not disclose the advertising nature of the engagement will now be definitively considered misleading (Article 16-N, §2), which may constitute a criminal offense under consumer protection statutes.

1.6. Scope of application and differentiated criteria

The exclusion of **email, private messaging and videoconferencing services in closed environments** from the scope of application of the duties had already been recognized by the STF (item 6 of the Thesis) and has now been incorporated into the MCI Decree (Article 16-O).

What is new?

The MCI Decree expressly provides for the possibility of adopting differentiated criteria for compliance with the duties set forth in Articles 16-A through 16-J and Article 16-M, taking into account factors such as the provider's economic size, level of interference in the circulation of content, risk of the activity and state of the art (Article 16-P). This flexibility indicates an attempt to calibrate the regulatory regime, especially to avoid disproportionate impacts on small providers.

Points to Watch

Even so, the effectiveness of this differentiation will depend on future regulation, especially regarding the concrete criteria for application and the form of oversight (Article 19-A).

1.7. Governance, self-regulation and oversight

The MCI Decree replicates the provisions of item 11 of the Thesis by reinforcing the importance of governance and self-regulation mechanisms, consolidating the requirement that providers adopt:

- terms and conditions that provide for notice-and-action systems and due process;
- transparency reports; and
- periodic reviews of such rules (Article 20-A).

Self-regulation is therefore considered a relevant element for demonstrating good faith in the assessment of potential violations (Article 20-A, §2).

What is new?

The MCI Decree expressly assigns to the ANPD regulatory and oversight powers related to providers' compliance with their duties (Article 19-A), expanding the agency's role in the digital ecosystem.

Points to Watch

In recent years, the ANPD has adopted a more active stance toward social media platforms. This movement was reinforced by the designation of the ANPD as the authority responsible for matters related to the Digital Child and Adolescent Statute ("ECA Digital") and the protection of children and adolescents in the online environment.

1.8. Record-Keeping Obligation

Beyond content moderation, the MCI Decree introduced a new obligation not provided for in the STF Thesis — which, at the time, was limited to the analysis of Article 19 of the MCI — by addressing the expansion of the record-keeping obligation.

The MCI already broadly required providers to retain connection records and records of access to internet applications, pursuant to Articles 13 and 15 of the statute. The MCI Decree, in turn, supplements this obligation by providing that the retention of IP address logs must also include the associated source logical port whenever this information is necessary to securely identify the originating terminal or the next point in the network (Article 15-A).

In practice, this means that providers must retain information in addition to the records they already maintain when the IP address alone is not sufficient to correctly identify the origin of a given connection or access.

The MCI Decree also establishes that the obligation to retain the source logical port does not depend on a prior request from an authority or interested third party and must be fulfilled independently by each provider (Article 15-A, §1). The disclosure of this information and the data linked to it, in turn, must follow the general MCI rules on the protection and disclosure of records, personal data and private communications, and must preserve the privacy, private life, honor and image of the parties directly or indirectly involved (Article 15-A, §2).

Points to Watch

To ensure compliance with this obligation, providers should verify whether their internal systems and procedures already allow for the retention of the source logical port whenever this information is necessary to correctly identify the origin of a connection or access.

Since the issue of logical ports has already arisen in discussions on content removal before Brazil's higher courts, it is also important to consider the potential legal impacts arising from a failure to provide this information, including in scenarios involving the imposition of fines or noncompliance with a court order.

2. DECREE ON THE PROTECTION OF WOMEN

The Decree on the Protection of Women establishes guidelines for the protection of women online and for combating violence against women in the digital environment. It will take effect sixty days after its publication (Article 15) and replicates several provisions of the MCI.

2.1. Duty of care and liability for systemic failure

Replicating the MCI Decree and the Thesis, internet application providers that act as intermediaries for third-party-generated content will be held liable in the event of a systemic failure to immediately disable access to content that constitutes crimes or unlawful acts committed against women because they are women (Article 4).

2.2. Notice-and-action system for illegal content

Providers must disable access to content that constitutes crimes or unlawful acts against women in the digital environment in response to notices (Article 5).

What is new?

The Decree on the Protection introduces a new obligation requiring providers to display the Ligue 180 hotline number in their own reporting channel (Article 5, §1).

In addition, providers must disable access, within two hours from the notice, to intimate content generated by third parties and displayed without authorization (Article 7, main section and §1).

2.3. Mitigation of coordinated digital harassment

Providers must adopt technical and proportionate measures to promptly reduce the reach and visibility of coordinated attacks against women that constitute gender-based violence (Article 8, main section). This obligation is independent of any prior notice or report: providers must act ex officio when they identify indicators of such occurrence (Article 8, §1).

The measures must be adopted on a priority basis in cases of political violence against women or where the victim is a woman with public visibility arising from her professional activities, such as members of the press (Article 8, §2).

What is new?

The duty to act ex officio to mitigate coordinated attacks (Article 8, §1) is a new obligation that goes beyond the reactive notice-based model provided for in the MCI Decree. In addition, the express prioritization of women with public visibility is also new (Article 8, §2).

2.4. Prohibition on the generation of intimate content by artificial intelligence

This Decree on the Protection of Women expressly prohibits internet application providers from generating or modifying third-party intimate content through the use of artificial intelligence or any other technological resource that alters the victim's image or voice (Article 9). Providers that offer artificial intelligence functionalities must implement technical and procedural safeguards to identify and block requests to generate such prohibited content (Article 10, main section), with implementation to be phased in and proportionate to the volume of access and the level of risk of the application (Article 10, sole paragraph). Detailed criteria will be established by regulation issued by the competent authority.

Points to Watch

The prohibition set forth in Article 9 is absolute and does not depend on notice: it covers any intimate content generated or modified by AI, including montages and deepfakes. However, the obligation under Article 10 to implement technical safeguards depends on future regulation by the competent authority. The ANPD, designated as the regulatory and oversight authority for the decree (Article 14), will play a central role in defining these parameters.

2.5. Retention and forwarding of information to public authorities

Article 12 establishes a **transitional regime** applicable until the competent authority regulates the matter. It is a provisional regime that sets minimum parameters while no specific regulation has been issued.

During this period, within the timeframe applicable to the case, the provider must either: **(i) remove the conten**t; or **(ii) inform the notifying party** of the grounds for maintaining it, as well as the available means to challenge the decision. In other words, the decree does not impose mandatory removal in all cases, allowing the content to remain available provided that there is a justification.

The timeframes vary according to the nature of the notified content:

- **2 (two) hours:** intimate content disclosed without authorization, pursuant to Article 7, §1;
- **6 (six) hours:** manifestly illegal content related to the crimes or unlawful acts set forth in Article 4, such as digital domestic violence, stalking, qualified threats, psychological violence and hate speech against women;
- **24 (twenty-four) hours:** all other cases of violence against women in the digital environment.

Finally, the sole paragraph of Article 12 regulates a subsequent step of the procedure: once a challenge is submitted to the provider, the provider must, within 24 (twenty-four) hours, restore or remove the content and communicate its decision to both the notifying party and the user responsible for the post.

Article 13, in turn, is structurally different: it does not address a removal timeframe, but rather a duty to preserve and cooperate in the production of evidence. Upon identifying or concluding that criminal or illegal content exists, the provider must retain and forward to public authorities the information that enables identification of authorship and materiality. This is an active obligation and does not depend on notice. The sole paragraph delegates to the Minister of Justice and Public Security the authority to regulate the manner of compliance, including which authority will receive this information.

3. DISCUSSION IN CONGRESS

The National Congress is discussing a Draft Legislative Decree challenging the decrees issued, arguing that the measures are unconstitutional, since it is the role of the Legislative Branch to regulate the matter. Accordingly, future discussions regarding implementation and entry into force may alter the proposed scenario.

b/luz

www.baptistaluz.com.br/