

Protection of women on The Internet

DECREE No. 12,976
OF MAY 20, 2026



DECREE NO. 12,976, OF MAY 20, 2026

Establishes guidelines for the protection of women on the internet and for combating violence against women in the digital environment

THE PRESIDENT OF THE REPUBLIC, in the exercise of the powers conferred upon him by Art. 84, caput, items IV and VI, subitem “a”, of the Constitution, and in view of the provisions of Law No. 12,965, of April 23, 2014,

DECREES:

**CHAPTER I
PRELIMINARY PROVISIONS**

Article 1. This Decree establishes guidelines for the protection of women on the internet and for combating violence against women in the digital environment.

Article 2. The following principles shall govern the regulatory, supervisory, and enforcement actions of the competent bodies and entities, as well as public policies aimed at preventing and combating violence against women in the digital environment:

I - non-discrimination on the basis of female gender, with all forms of violence, intimidation, or degrading exposure committed in the digital environment being prohibited;

II - victim-centered approach, ensuring adequate support, the preservation of evidence, the availability of accessible reporting channels, and the adoption of measures to cease or mitigate harm;

III - protection of data and privacy, ensuring the inviolability of women’s intimacy, private life, honor, and image;

IV - non-revictimization, prohibiting further exposure of women by competent authorities and internet application providers for the purpose of adopting measures to cease or mitigate harm; and

V - recognition of discrimination based on multiple criteria as an aggravating factor in violence against women.

Article 3. For the purposes of this Decree, the following definitions apply:

I - intimate content - an image, video, audio recording, text message, or any written content, or a combination thereof, that depicts nudity, partial nudity, a sexual act, or a sexualized context, even if produced and manipulated, in whole or in part, by an artificial intelligence system or equivalent technological means; and

II - violence against women in the digital environment - crimes or unlawful acts against women, on the basis of their female gender, consisting of an act, conduct, or omission that causes death, harm, or physical, sexual, psychological, political, or economic suffering, including property damage, in any sphere of their lives, committed, instigated, facilitated, or aggravated, in whole or in part, by the use of digital technologies, such as:

a) domestic and family violence against women, including psychological violence, pursuant to the provisions of Article 7, *caput*, item II, of Law No. 11,340, of August 7, 2006, perpetrated through messages, posts, digital stalking, online surveillance, isolation, or any other form of technological control;

b) political violence against women perpetrated in a digital environment, pursuant to the provisions of Article 326-B of Law No. 4,737, of July 15, 1965 — Electoral Code, which includes harassment, embarrassment, humiliation, persecution, or threats against female candidates or holders of elective office;

c) aggravated threats against women on the basis of their female gender, pursuant to the provisions of Article 147, Paragraph 1, of Decree-Law No. 2,848, of December 7, 1940 – Penal Code;

d) stalking of women carried out through digital means, pursuant to the provisions of Article 147-A of Decree-Law No. 2,848, of December 7, 1940 – Penal Code, including through monitoring of social media, repeated sending of messages, and use of tracking technologies;

e) psychological violence against women, pursuant to the provisions of Article 147-B of Decree-Law No. 2,848, of December 7, 1940 – Penal Code, including when perpetrated through the use of artificial intelligence or technological means that alter the victim's image or sound;

f) dissemination of scenes of sex, nudity, or lewd acts without consent via the internet, pursuant to the provisions of Article 218-C of Decree-Law No. 2,848, of December 7, 1940 – Penal Code;

g) unauthorized recording of scenes of nudity or sexual or lewd acts of an intimate and private nature, pursuant to the provisions of Art. 216-B of Decree-Law No. 2,848, of December 7, 1940 – Penal Code, including through editing or the use of artificial intelligence;

h) digital sexual harassment, pursuant to the provisions of Article 215-A of Decree-Law No. 2,848, of December 7, 1940 – Penal Code; and

i) crimes committed via the internet that disseminate content propagating hatred or aversion towards women, pursuant to the provisions of Article 1, caput, item VII, of Law No. 10,446, of May 8, 2002.

CHAPTER II

PROTECTION OF WOMEN IN THE PROVISION OF INTERNET APPLICATIONS

Section I

DUTY OF CARE IN CASES OF CRIMES AGAINST WOMEN OR GROUPS OF WOMEN

Article 4. Internet application providers that act as intermediaries for content generated by third parties shall be held liable in the event of a systemic failure to immediately remove content that constitutes crimes or unlawful acts committed against women on the basis of their female gender, pursuant to the provisions of:

I - Articles 141, paragraph 3, 146-A, 147, paragraph 1, 147-A, and 147-B of Decree-Law No. 2,848, of December 7, 1940 – Penal Code;

II - Article 1, caput, item VII, of Law No. 10,446, of May 8, 2002;

III - Law No. 11,340, of August 7, 2006; and

IV - Law No. 14,192, of August 4, 2021.

Paragraph 1. An internet application provider shall be deemed to have committed a systemic failure if it fails to demonstrate the adoption of adequate measures to prevent or remove the criminal or unlawful content referred to in the *caput* that:

I - provide, in accordance with the state of the art, the highest levels of security for the type of service offered; and

II - inhibit the widespread circulation of the content referred to in items I to IV of the *caput*.

Paragraph 2. The existence of criminal or unlawful content in isolation does not, in and of itself, constitute a systemic failure.

Paragraph 3. Internet application providers that act as intermediaries for content generated by third parties shall make available to the competent authorities the information and data necessary to verify the adoption and application of the measures referred to in paragraph

Section II

REPORTING ACTS OF VIOLENCE AGAINST WOMEN IN THE DIGITAL ENVIRONMENT

Article 5. Without prejudice to the provisions of Article 4, internet application providers that act as intermediaries for third-party-generated content shall, in response to notifications, remove content that constitutes crimes or unlawful acts against women in the digital environment.

Paragraph 1. In the space provided by the provider for submitting the notification, a notice shall be displayed, in a clear and user-accessible manner, containing the telephone number and contact channels of the Women's Assistance Hotline – Dial 180.

Paragraph 2. For the purposes of the provisions in the caput, the notification submitted through an official and dedicated channel provided by the internet application provider shall be valid.

Paragraph 3. The competent authority may regulate:

- I - the form of notification and counter-notice;
- II - the deadline for removing the content and for responding to the notifying party;
- III - those entitled to file a notification;
- IV - the deadline for the responsible party to file a counter-notice; and
- V - any other necessary procedures.

Paragraph 4. The notification regarding criminal or unlawful content shall contain, under penalty of nullity:

- I - elements that allow for the identification of the possible illegality or unlawfulness;
- II - information that allows for the specific identification of the criminal or unlawful content to be removed; and
- III - identification of the notifying party and, where applicable, an indication of the basis for their standing.

Paragraph 5. The provider may keep the content available if, following a diligent and reasoned analysis, it concludes that there is reasonable doubt regarding the criminal or unlawful nature of the content, taking into account the proportionality between the doubt and the severity of the crime or unlawful act; in such cases, the provider shall communicate to the notifying party the reasons for not removing the content.

Article 6. Upon receipt of a notification, the internet application provider shall:

- I - confirm receipt of the notification to the notifying party; and
- II - evaluate the content of the notification and take the appropriate measures, observing the following:

a) in the event of removal, the internet application provider shall communicate the decision to the notifying party and to the user who published the content, and shall inform them of the specific grounds for the removal and the means to challenge it;

b) in the event of non-removal of the content subject to notification, the internet application provider shall communicate the decision to the notifying party and shall inform them of the specific grounds for maintaining the content and the means to challenge it; and

c) in the event of reconsideration following a challenge, the internet application provider shall communicate the decision to the user who published the content and to the notifying party, providing the respective grounds.

Section III

REMOVAL OF INTIMATE CONTENT GENERATED BY THIRD PARTIES

Article 7. Internet application providers shall remove the unauthorized display of intimate content generated by third parties, within the scope of their services, upon notification.

Paragraph 1. The removal referred to in the *caput* shall occur within a period not exceeding two hours from the notification.

Paragraph 2. The notification referred to in the *caput* shall be made by the victim or their representative, providing the notifying party's identification information and elements specifying the intimate content to be removed.

Paragraph 3. On behalf of the victim, the following may submit the notification referred to in the *caput* and paragraph 1:

I - retained attorneys;

II - law enforcement authorities;

III - the Federal Public Prosecutor's Office;

IV - the State Public Prosecutor's Offices;

V - the Public Prosecutor's Office of the Federal District and Territories;

VI - the State Public Defender's Offices and the Federal District Public Defender's Office; and

VII - the Federal Public Defender's Office.

Paragraph 4. Intimate content shall be removed from the entire application and digitally fingerprinted so that its re-upload is automatically blocked, as established by regulation issued by the competent authority.

Paragraph 5. Internet application providers shall make available a specific, permanent, free, prominent, and easily accessible space dedicated to the receipt of notifications and processing of complaints regarding intimate content, with confirmation of receipt and the possibility for the victim or their representative to track the case.

Section IV

DUTY TO MITIGATE REACH AND VISIBILITY IN CASES OF DIGITAL HARASSMENT

Article 8. Internet application providers that act as intermediaries for third-party-generated content shall adopt technical and proportionate measures to promptly reduce the reach and visibility of coordinated attacks against women that constitute violence against women.

Paragraph 1. The provisions of the *caput* apply regardless of prior notification or complaint by the victim, and the internet application provider shall act *ex officio* upon identifying indicators of such occurrences.

Paragraph 2. The measures provided for in this Article shall be adopted as a matter of priority in cases of political violence against women or when the victim is a woman with public exposure arising from her professional activities, such as media professionals, especially when acts of violence, intimidation, or harassment are intended to coerce, silence, restrict her public participation, or compromise the exercise of her professional activities.

CHAPTER III

GENERATION AND ALTERATION OF INTIMATE CONTENT BY ARTIFICIAL INTELLIGENCE OR ANY OTHER TECHNOLOGICAL MEANS

Article 9. Internet application providers are prohibited from generating or altering intimate content of third parties through the use of artificial intelligence or any other technological means that alters the victim's image or sound.

Article 10. Internet application providers based on artificial intelligence functionalities or equivalent technological means shall implement technical and procedural safeguards to identify and block requests for the generation of content prohibited by the provisions of Article 9, as established by regulation by the competent authority.

Sole Paragraph. The mechanisms referred to in the *caput* shall be implemented in a phased manner and in proportion to the volume of traffic and the risk level of the application.

CHAPTER IV

INTEGRATED SYSTEM FOR THE PREVENTION, PROTECTION, AND SUPPORT OF WOMEN VICTIMS OF VIOLENCE IN THE DIGITAL ENVIRONMENT

Article 11. An act of the Minister of State for Justice and Public Security shall establish an interministerial working group for the purpose of drafting a proposal for the creation, structuring, and implementation of an integrated system for the prevention, protection, and support of women victims of violence in the digital environment.

Paragraph 1. The act referred to in the *caput* shall provide for the composition, powers, mode of operation, and mechanisms for public participation in the interministerial working group.

Paragraph 2. Representation of the following bodies shall be guaranteed in the composition of the interministerial working group referred to in the *caput*:

I - Ministry of Women; and

II - Secretariat of Social Communication of the Presidency of the Republic.

CHAPTER V

FINAL AND TRANSITIONAL PROVISIONS

Article 12. Until regulations are issued by the competent authority, and without prejudice to the period of up to two hours for the removal of third-party generated intimate content provided for in Article 7, paragraph 1, internet application providers have a duty to remove the content or communicate to the notifying party the grounds for maintaining it and the appropriate means to challenge it, in accordance with the following timeframes, counting from the notification:

I - six hours, in cases of manifestly illegal content that characterizes the crimes or unlawful acts referred to in the *caput* of Art. 4; and

II - twenty-four hours, in all other cases of violence against women in the digital environment.

Sole paragraph. Upon receipt of the challenge referred to in the *caput*, the internet application provider shall, within a period not exceeding twenty-four hours:

I - restore or remove the content; and

II - communicate the decision to the notifying party and to the user who published the content.

Article 13. Internet application providers, upon identifying or concluding the existence of content related to crimes or unlawful acts, shall ensure the preservation and forwarding of the information necessary to identify its authorship and materiality to the Public Authorities.

Sole Paragraph. An act of the Minister of State for Justice and Public Security shall regulate the manner of compliance with this Article, including the possibility of forwarding the information referred to in the *caput* to the body responsible for receiving, processing, and making it available to the competent authorities, subject to the constitutional and legal powers of the federal entities.

Article 14. The regulation, oversight, and investigation of violations covered by this Decree are the responsibility of the National Data Protection Agency (ANPD), pursuant to the provisions of Article 19-A of Decree No. 8,771, of May 11, 2016.

Article 15. This Decree shall enter into force sixty days after the date of its publication.

Brasília, May 20, 2026; the 205th year of Independence and the 138th year of the Republic.

Luiz Inácio Lula Da Silva

Wellington César Lima e Silva

Márcia Helena Carvalho Lopes

Sidônio Cardoso