OAS | MESECVI

INTER-AMERICAN MODEL LAW

to Prevent, Punish, and Eradicate Gender-Based Digital Violence against Women

FOLLOW-UP MECHANISM
BELÉM DO PARÁ CONVENTION (MESECVI)
Twenty-Second Meeting of the Committee of Experts
December 9 and 10, 2025
Fortaleza, Brasil

OEA/Ser.L/II/7.10
MESECVI/CEVI/doc.299/25
December 10, 2025
Original: Spanish

INTER-AMERICAN MODEL LAW TO PREVENT, PUNISH, AND ERADICATE GENDER-BASED DIGITAL VIOLENCE AGAINST WOMEN[1][2]

[1] For the purposes of this Law, the term gender-based digital violence against women includes the terms "technology-facilitated gender-based violence against women", "online/digital violence against women" and cyberviolence against women, which have been used interchangeably in various laws across the region.

[2] This Model Law has been drafted to reflect the legal and linguistic context of the English-speaking Caribbean States Parties to the Belém do Pará Convention. It is not a literal translation of the Spanish version.

The Committee of Experts of the Follow-up Mechanism to the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women – Convention of Belém do Pará – (CEVI), meeting within the framework of the XXII Meeting of the CEVI, recognizing that violence against women constitutes a violation of human rights and a historical manifestation of unequal power relations between women and men, and affirming that all women, in all their diversity, have the right to a life free from violence both in physical spaces and in digital environments;

Recalling that since 1994 the Convention of Belém do Pará has established a clear and continuing obligation of States to act with due diligence to prevent, investigate, and punish violence against women, and that this obligation was framed in response to all forms of systemic violence, that occur across public and private settings and is reproduced, more recently, in digital environments and platforms, social media, instant messaging services, surveillance and data extraction systems, and emerging technologies with massive reach, among others;

Highlighting that the IX Conference of States Parties to the MESECVI reaffirmed the urgent need to strengthen ties between the MESECVI and civil society, including feminist and digital rights organizations that have documented and confronted gender-based digital violence in all its complexity, and that such collaboration is essential for the development and implementation of effective transformative public policies in this area;

Taking note of the MESECVI Strategic Plan 2024–2029, which identifies emerging forms of violence, including digital violence against women, as a hemispheric priority and calls upon States to adopt coherent normative frameworks, comprehensive public policies, and protection mechanisms incorporating an intersectional, technopolitical, and human rights–based perspective, as well as to allocate sufficient resources to ensure their effective and sustained implementation;

Considering that technological acceleration, the pervasive digitalization of daily life, the concentration of power in transnational private platforms and other internet intermediaries, and the instrumental use of technologies to monitor, control, expose, harass, silence, or harm women reproduce, amplify, and often perpetuate structural patterns of gender-based violence, ignoring geographic boundaries and generating/inflicting immediate and irreparable harm;

Noting with particular concern that historical forms of violence against women, including physical, psychological, sexual, economic, political, among others, have found new forms of expression, expansion, and replication in digital environments, and that digital violence against women is neither isolated nor is it a recent phenomenon, but part of a continuum of patriarchal violence that cuts across all spheres of life and whose impact extends to women's bodies, reputations, safety, public participation, freedom of expression, and the exercise of citizenship and political rights;

Observing that digital violence against women is a distinct and pervasive form of gender-based violence, insofar as it leverages digital technologies to generate a differentiated impact and disproportionately affect women because they are women, and that has the purpose or effect of undermining or harming their dignity, reputation, autonomy, and security, giving rise to violent, hostile, and unsafe digital environments;

Emphasizing that manifestations of digital violence may be accompanied, linked, or interconnected with other forms of gender-based violence outside the digital environment, demonstrating its continuity and cross-cutting nature across both digital and non-digital spheres;

Recognizing that digital violence manifests, in various ways, such as threats, repeated harassment, hate and smear campaigns, online sexual harassment, digital extortion, obtaining, dissemination, and/or manipulation of intimate images without consent, abusive monitoring and surveillance, identity theft, the theft and publication of personal and sensitive data, coercive technological control, incitement to physical or sexual violence, coordinated attacks to silence women's voices and those of human rights defenders, racist and misogynistic attacks targeting Afro-descendant, Indigenous, migrant, young, and disabled women, trans women, as well as disinformation and defamation campaigns aimed at expelling women from public and political spaces;

Bearing in mind that these practices constitute a form of gender-based discrimination that limits, restricts, or nullifies the enjoyment and exercise of fundamental human rights, including the right to life, to live free from violence, to physical, psychological, and/or sexual integrity, to freedom of expression and association, to privacy, to the integrity and availability of data and information systems, to honor and dignity, to political and public participation, and to defend human rights;

Reaffirming that, today, digital environments are spaces for socialization, political organization, cultural creation, education, employment, access to services, and the exercise of freedom of expression, and that guaranteeing women's digital safety is therefore essential for the exercise of democratic citizenship and for the very validity of the rule of law in the Americas;

Taking note that digital violence against women performs a disciplining function: it seeks to punish bodily and sexual autonomy, sanction women who report violence, criminalize the defense of rights, discourage public participation, and intimidate women who occupy positions of political, judicial, journalistic, community, artistic, academic, trade union, or territorial leadership, among others, reproducing silencing patterns that undermine democracy itself;

Recognizing that there are differentiated and aggravated impacts on groups of women and girls historically subjected to multiple forms of intersectional discrimination, including Indigenous, Afro-descendant, older women, young women, migrants, refugees, women with disabilities, rural and peasant women, women in contexts of mobility, as well as environmental and territorial women defenders, journalists, community leaders, human rights defenders, and digital activists, and underscoring that in many cases digital violence reproduces colonial, racist, and misogynistic stereotypes that seek to delegitimize their political and social leadership;

The Model Law recognizes the violation of the collective right to the spiritual and cultural integrity of women and their communities in digital environments, from a gender and intersectionality-based perspective, and the need to establish protective frameworks to safeguard it. Spiritual violence is understood as violence frequently perpetrated against Indigenous women, girls and adolescents, which infringes upon the collective rights of their

communities as reflected in their spiritual and cultural practices, their relationship with their territories and the environment, and their sacred sites;

Considering that unequal access to adequate infrastructure, gender-responsive digital literacy, and effective reporting and redress mechanisms deepen the vulnerability experienced by broad sectors of women in the region, particularly in contexts of poverty, territorial exclusion, digital divides, and forced displacement;

Bearing in mind the need to highlight the differentiated impacts this issue generates for girls and adolescents, who, by engaging early and continuously in digital environments as part of their socialization, education, and participation, are particularly exposed to risks associated with technology use, including those facilitating trafficking, sexual exploitation, grooming, harassment, and other forms of digital violence;

Underlining that the reinforced duty of due diligence required of States by the Convention of Belém do Pará obliges the States to prevent, investigate, punish, and repair all forms of violence against women, including those committed, instigated, aggravated, or mediated through digital technologies, and that this duty requires adopting updated normative frameworks, comprehensive public policies, urgent protection mechanisms, effective judicial and administrative remedies, and guarantees of non-repetition that address structural causes of violence;

Recalling that the Inter-American Model Law to Prevent, Punish, and Eradicate Violence against Women in Political Life recognized that political violence aims to exclude, discredit, or intimidate women participating in public life and that such violence can also occur through digital means, including harassment, defamation, exposure of intimate information, and sexist hate speech; and highlighting the need to consolidate and expand that understanding in this instrument so that digital attacks aimed at discouraging or punishing women's participation in democratic life are addressed as serious forms of gender-based violence and illegitimate restrictions of political rights;

Echoing that the Inter-American Model Law on Femicide/Feminicide developed the notion of State responsibility for extreme forms of violence against women, emphasizing the need to integrate structural discrimination, social tolerance patterns, and failures in State due diligence into the institutional response; and noting that digital violence may constitute a link within that continuum which, in contexts of impunity and escalating risk, may lead to lethal physical violence;

Recognizing the legitimacy and centrality of the voices of women and girls who have survived digital violence, who have faced non-consensual exposure of intimacy, hate and defamation campaigns, threats of death or sexual violence, and digital persecution that translates into fear, self-censorship, job loss, expulsion from educational or work environments, disruption of community ties, and forced displacement also in physical spaces;

Bearing in mind the historical, technical, and political contributions of feminist and digital rights organizations in the region, including networks of human rights defenders, collectives of women journalists and communicators, organizations of Indigenous and Afro-descendant women, organizations working on sexual and reproductive autonomy, and grassroots digital violence response collectives that documented, denounced, and named digital forms of violence long before their institutional recognition;

Highlighting that thanks to the leadership of women's organizations in the region, the Americas have become a global reference in the creation and adoption of regulatory frameworks to confront digital violence, in this regard, we acknowledge in particular, the contribution of the *Ley Olimpia* movement and Digital Defenders, who, drawing on their own experiences as survivors, have been pioneers in conceptualizing digital violence and generating legal frameworks that make visible the non-consensual distribution, storage, and circulation of intimate material, digital sexual extortion, and online harassment as specific forms of gender-based violence that harm women's integrity, dignity, mental health, reputation, and life prospects, requiring responses from the States that recognize both the magnitude of the harm and the urgency of protection, timely removal of content, adequate sanctions, and comprehensive reparations; they have also pointed out the patriarchal algorithm and the responsibility of platforms in the reproduction of this violence and provided comprehensive support to hundreds of victims across the Americas. That is why we rely on this important, living movement to continue the progress towards better regulations and for the implementation of this Model Law;

Taking note that these initiatives arise from the determination of the women who suffered and survived digital violence, and transformed it into a collective demand for eradication, along with other civil society movements and organizations, and have emphasized not only the criminal dimension but also the need for prevention, gender-responsive digital education, mandatory training for justice operators and security forces, rapid response protocols, urgent protection measures, and accessible, stigma-free, and culturally appropriate pathways to justice;

Noting that human rights defenders—including journalists and territorial, environmental, community, trade union, Afro-descendant, and Indigenous defenders—have been subjected to systematic digital attacks aimed at delegitimizing their work, normalizing violence against them, and enabling hostile environments that facilitate subsequent physical aggressions, and that this dynamic, when tolerated or reproduced by State actors or private actors with public influence, generates international responsibility for the State;

Emphasizing that technological innovation must be accompanied by clear and effective regulatory frameworks, as digital violence, like physical violence, requires decisive State action and the active participation of all actors involved in its prevention, response, punishment, and reparation;

Warning that existing legal frameworks in many States Parties have not yet incorporated comprehensive definitions of gender-based digital violence, nor have they established clear obligations for digital platforms and other internet intermediaries regarding prevention, timely removal of violent or non-consensual content, preservation of evidence, cooperation with investigations, and enhanced due diligence in high-risk situations, and noting that the absence of regulation or normative adaptation creates zones of impunity and revictimization that perpetuate violence;

Promoting an inclusive model of digital governance, based on active and shared participation among multiple stakeholders, including States, internet intermediaries, civil society, academia, and women's and feminist movements, who must converge in joint actions to prevent, address, punish, and repair gender-based digital violence; and recognizing that such multi-stakeholder articulation will foster the governance and creation of safe and democratic

digital environments, strengthen accountability, and support the development of public policies that integrate gender equality, human rights protection, and digital justice as pillars for transformation in the Americas;

Underscoring the need to ensure that the response to digital violence against women does not compromise their fundamental rights nor become a tool for censorship or persecution aimed at silencing, dissenting, opposing, or critical voices, as this would violate freedom of expression and disproportionately affect women journalists, activists, human rights defenders, environmental defenders, and defenders of sexual and reproductive rights;

Recognizing the need to develop common inter-American standards to guide legislative adaptation, close normative gaps, and facilitate cooperation among States, organs of the Inter-American System, civil society, academia, the technology sector, and multilateral organizations to address digital violence as a hemispheric phenomenon that transcends national borders and requires coordinated responses with independent judges and magistrates, who must ensure that all interpretation and application of this Law complies with international human rights standards;

Considering that monetization models based on increasing traffic and content dissemination, even when shared without consent, have facilitated practices that allow economic profit from the creation, dissemination, or commercialization of misogynistic or violent digital content, turning the harm and exposure of victims into sources of revenue, and that it is therefore necessary to strengthen the responsibility and due diligence of internet intermediaries, ensuring effective mechanisms for prevention, response, and reparation, as well as governance frameworks that prioritize the safety and dignity of women over economic interests;

Underlining the obligation of States to guarantee access to justice mechanisms that are impartial, independent, timely, culturally appropriate, accessible for women with disabilities, cost free when necessary, and free from harmful stereotypes such as racial, gender-based, or ableist biases, among others, and affirming that justice systems must be equipped to investigate, preserve digital evidence, protect victims and survivors, and punish those responsible for acts of digital violence;

Taking into account that gender-responsive digital literacy and autonomy are essential components of prevention and the construction of full digital citizenship, and that education in digital environments must include respect for bodily and sexual autonomy, understanding of consent, the elimination of stereotypes and myths that blame victims, and the promotion of egalitarian, respectful, and non-violent relationships in the digital sphere;

Warning that the absence of safe digital environments limits women's political participation, discourages access to public office and decision-making processes, restricts the reach of their voices in democratic debate, and constitutes a contemporary form of exclusion and silencing incompatible with democratic principles and with the right of women to participate equally in public and political life;

Recognizing that the response to gender-based digital violence must engage all actors and be multidimensional—preventive, protective, punitive, and reparative; that it must include clear protocols for public institutions; enhanced due diligence policies in the private sector; immediate attention mechanisms and psychosocial, legal, and community support for victims

and survivors; and comprehensive reparation strategies recognizing physical, psychological, emotional, reputational, political, economic and community harm;

Aware that digital technologies can also serve as tools for empowerment, access to information, reporting, political organization, collective memory-building, and human rights advocacy, and affirming that women have the right to appropriate these technologies critically and safely, in conditions of freedom, dignity, autonomy, and security, without fear of retaliation, persecution, or violence;

Convinced that States must guarantee that women and girls, in all their diversity, have the right to inhabit, create, express themselves, participate, love, learn, engage in political organizations, and defend human rights in digital environments free from violence, discrimination, persecution, and gender-based censorship;

Adopt this Inter-American Model Law to Prevent, Punish, and Eradicate Gender-Based Digital Violence against Women as a normative, political, and educational tool intended to guide legislative harmonization, the design of public policies, diligent action by justice systems, inter-State cooperation, private-sector responsibility, and the strengthening of community and feminist capacities to protect and guarantee the right of all women and girls to a life free from violence—including in digital environments.

CHAPTER I
DEFINITION AND SCOPE OF APPLICATION

Article 1. Object

The purpose of this law is to ensure the prevention, response, protection, investigation, punishment, reparation of harm and the eradication of gender-based digital violence against women[3], occurring both in the public or private sphere, and whether committed, instigated, facilitated, or aggravated in whole or in part through the use of digital technologies. Such violence may be exacerbated by conditions such as sexual orientation and gender identity, ethnic and racial origin, among other factors of vulnerability.

Article 2. Definition of Gender-Based Digital Violence Against Women

Any action, conduct, or omission directed against women, based on gender, that causes death, harm, or physical, sexual, psychological, political, or economic suffering, including damage to property, committed in any sphere of their lives, and which is perpetrated, instigated, facilitated, or aggravated, in whole or in part, through the use of digital technologies. The specific manifestations of such violence are set forth in Article 7 of this law.

Article 3. Scope of Protection

Gender-based digital violence against women manifests through the ongoing interconnection between digital technologies and women's everyday interactions in the physical world. It is therefore intertwined with and subject to continuous transformation, such that it may shift from the digital to the physical realm and vice versa.

This Law shall apply to acts of digital violence that:

a. Occur in private settings, within any interpersonal relationship, including familial, intimate partner or former partner relationships, regardless of whether or not the aggressor shares the same residence as the woman;

b. Occur in public or collectively accessible spaces or are perpetrated, condoned, or committed with the acquiescence of the State or its agents.

Such acts of violence may be committed by individuals known or unknown to the victim, acting alone or in concert with others.

Article 4. Guiding Principles

This law recognizes that women's right to live free from gender-based digital violence encompasses the rights to life, personal integrity, autonomy, comprehensive development,

[3] For the purposes of this Law, the term "women" shall refer to women, girls, and adolescents, as well as any person who self-identifies as a woman in all her diversity, in accordance with Article 9 of the Belém do Pará Convention.

participation in public life and privacy, and affirms that it is a shared responsibility of the State and internet intermediaries to ensure the full exercise of this right through adherence to the following guiding principles:

a. Equality, equity and non-discrimination;
b. Heightened due diligence;
c. Best interest of girls and adolescents;
d. Progressivity of human rights and prohibition of retrogression;
e. Comprehensive protection;
f. Confidentiality;
g. Digital governance;
h. Protection of the right to information and freedom of expression;
i. Victim-centered approach;
j. International cooperation and collaboration;
k. Transparency;
l. Security with a human rights-based approach;
m. Human dignity;
n. Non-revictimization and trauma-informed approach;
o. Multidisciplinary State intervention;
p. Intersectionality;
q. Proportionality, necessity, and legality.

Article 5. Definitions

a. Algorithmic Bias or Prejudice: Occurs when systematic errors in machine learning algorithms result in discriminatory outcomes due to flaws or inherent characteristics in the system's design. It also arises when an artificial intelligence system makes a prediction that leads to unfair outcomes or adverse treatment for an individual or group of individuals.

b. Internet Intermediaries: Internet intermediaries range from service providers[4] to search engines, and include social networking platforms, digital platforms, e-commerce platforms, and web servers[5].

c. Content Moderation: Activities carried out by internet intermediaries, whether automated or not, aimed in particular at preventing, detecting, identifying, and acting upon illegal content or information that violates their terms of service.

[4] For the purposes of this Law, "service providers" shall be understood in accordance with the definition established in the Council of Europe's Convention on Cybercrime (2001): ""service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service."

[5] Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Special Report on Digital Inclusion and Internet Content Governance, OEA/Ser.L/V/II. CIDH/RELE/INF. 28/24 (2024), *See*: https://www.oas.org/en/iachr/expression/reports/Digital_inclusion_eng.pdf

d. Content Curation: Refers to the process through which digital platforms select, organize, and present information to users, determining the visibility of content in main feeds, search results, and personalized recommendations. Unlike content moderation, content curation is driven by algorithmic or commercial criteria generally unknown to the public, with significant effects on access to information and opinion formation.

e. Gendered Disinformation: Refers to the deliberate and coordinated dissemination of false or misleading content that, based on gender bias, stereotypes, sexism, misogyny, and patriarchal cultural and social norms, aims to threaten, intimidate, and silence women. This practice constitutes a public issue that seriously undermines freedom of expression and the public and political participation of women, girls, and adolescents.

f. Dissemination of False Content: Refers to the deliberate and intentional mass dissemination of information known to be false.

g. Global Annual Revenue: Refers to the total income obtained by an internet intermediary in a fiscal year, derived from its commercial activities worldwide, before deducting taxes and other expenses.

h. Digital Environments/Spaces: Refers to the virtual space in which information is created, exchanged, and consumed, encompassing online interactions, digital services, and the governance frameworks that regulate them. These environments include both regulated and unregulated or weakly supervised spaces.

i. Gender Digital Divide: Refers to the disparities in the design, use, access, development, impact, decision-making, and benefits derived from digital technologies between men and women. Gender stereotypes and gender-based digital violence against women exacerbate and perpetuate this divide.

j. Intimate/Sexual Nature: Refers to the dimension of private life and sexuality of a person, involving aspects of autonomy, consent, and dignity, that does not relate to a matter of public interest.

k. Misogynistic Content: Content prohibited under this law that promotes or incites hatred, rejection, aversion, contempt, and violence against women, and that may cause harm or suffering, based on their gender.

l. Consent: The right to individual self-determination, grounded in the constitutional-legal framework of liberty. For the purposes of this law, consent shall be deemed absent when the following elements are present: i. Use or threat of use of force; ii. Coercion or fear of violence or its consequences; iii. Intimidation, meaning conduct or circumstances that pose a threat to the life or safety of the victim or a third party; iv. Psychological oppression, which occurs when there is a relationship between the victim and the perpetrator involving emotional or psychological ties; v. Abuse of

power, where the perpetrator holds a position of authority or influence over the victim[6].

m. Digital Governance: The development and complementary application, by governments, statutory bodies, the private sector, civil society, and the technical community, in their respective roles, of shared principles, norms, rules, decision-making procedures, and activities that shape the evolution and use of the Internet[7].

n. Perpetrator: For the purposes of this law, a perpetrator is understood to be any person who commits acts of gender-based digital violence against women, either directly or through third parties or other technological means.

Article 6. Women's Right to Live Free from Gender-Based Digital Violence

This right encompasses, among others, the following:

a. Equality and non-discrimination;
b. Protection of their physical, psychological, and emotional integrity against any form of gender-based digital violence;
c. Personal liberty and security, including the right to participate in digital spaces without fear of retaliation;
d. A dignified life, including in digital environments;
e. Freedom from cruel, inhuman, or degrading treatment in digital environment;
f. Use and control their own image and to build their own digital identity, free from discrimination;
g. Respect for digital identity;
h. To live free from all forms of sexual harassment;
i. Freedom of expression, assembly, and association in digital spaces, ensuring full access to, use of, and participation in technology;
j. Anonymity or pseudonymity to protect their identity in digital spaces, if they so choose, subject to limitations based on potential harm;
k. Access to justice, ensuring fair and effective procedures and transformative remedies in cases of digital violence;
l. Active participation in political and public life, including equal access to public functions in their country and the ability to engage in public affairs through digital platforms and tools;
m. Freedom to practice one's religion and spiritual beliefs without fear of reprisal in digital spaces;

---

[6] The concept of consent shall be interpreted in accordance with the provisions established by the Committee of Experts of the MESECVI in its General Recommendation No. 3: The concept of consent in cases of sexual violence against women for gender reasons. *See*: https://belemdopara.org/wp-content/uploads/2022/03/consentimiento_220322_eng.pdf

[7] *See* United Nations Educational, Scientific and Cultural Organization (UNESCO). (2023). *Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach*. https://unesdoc.unesco.org/ark:/48223/pf0000387339

n. Privacy, confidentiality, security, integrity, availability and protection of personal data, even in the absence of data protection laws or related regulatory frameworks[8];
o. To rectify, erase, or limit the processing of personal data, in accordance with the principle of self-determination and control over such data;
p. Protection against disinformation or the dissemination of content that undermines their life, dignity, reputation, or safety, or that promotes harmful stereotypes perpetuating violence and discrimination;
q. To object to data processing, particularly where based on profiling, and to be informed about automated decision-making and its consequences;
r. To be informed about the digital regulation of content that affects them, with clear and detailed information that facilitates decision-making;
s. Education and digital literacy free from stereotyped patterns and behaviors, as well as social and cultural practices based on concepts of inferiority or subordination, to ensure inclusion, the guarantee of rights, and development in the digital environment;
t. Free access to information, services, and technological resources, without undue censorship by State or private actors.

Article 7. Manifestations of Gender-Based Digital Violence Against Women

In accordance with the definition provided in Article 2, manifestations of gender-based digital violence against women include, but are not limited to, the following:

7.1. Manifestations of gender-based violence against women's rights to life, and to physical, psychological, and/or sexual integrity

a. Inducing, coercing, or facilitating the suicide of a woman, or assisting her in committing suicide, through the use of digital technologies;

b. Exposing, disseminating, distributing, commercializing, or exchanging photographs, images, videos, or audio recordings of an intimate/sexual nature without the consent of the woman depicted therein, whether such materials are real, generated or altered through artificial intelligence, digital applications, technological programs, or any internet intermediary that facilitates such actions;

c. Possessing, storing, or distributing sexual violence material involving women, by obtaining, retaining, or sharing such content in any digital format or medium;

d. Recruiting, coercing, or threatening women through digital technologies for the purposes of sexual abuse or exploitation, trafficking, slavery, or forced prostitution, whether in the digital sphere or beyond;

[8] OAS/Ser. CJI/doc.638/21, Updated Principles of the Inter-American Juridical Committee on Privacy and Personal Data Protection, with annotations; *See*: https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf

e. Harassing, monitoring or surveilling a woman through digital technologies, devices, products or services, in an unwanted, repeated, and persistent manner with the intent to cause distress or intimidation;

f. Engaging in repeated conduct involving graphic, audio, or audiovisual content with the intent to intimidate, threaten, or undermine a woman's self-esteem or reputation, including the unsolicited sending of sexually explicit materials, propositions, or insinuations;

g. Organizing hostile attacks against the physical, psychological, and/or sexual integrity of a woman or group of women involving the coordinated participation of multiple individuals or user accounts in digital environments;

h. Implementing, designing, or using algorithms, artificial intelligence, automated decision-making systems, or digital tools that generate, reproduce, or amplify discriminatory biases against women on the basis of gender, facilitate the dissemination of explicit violent content against women, or promote violence against women;

i. Profiting from the creation, dissemination, or commercialization of misogynistic digital content, including non-consensual images, audio, videos, or materials generated by artificial intelligence, which promote, reproduce, or normalize violence against women and/or discriminatory gender stereotypes.

7.2. Manifestations of gender-based violence against women's rights to privacy, integrity, and the availability of data and information systems

a. Producing, distributing, and/or circulating graphic, audio, or video content that violates a woman's control over her privacy and personal data;

b. Accessing and/or impersonating a woman through digital technologies to unlawfully obtain her personal information;

c. Installing tracking devices in vehicles, personal belongings, or other items without the woman's consent;

d. Using applications or installing spyware on electronic devices to gain unauthorized access and exert control over a woman's privacy, among others, via remote access to cameras, microphones, or geolocation functions.

7.3. Manifestations of gender-based violence against women's rights to honor, dignity, and public participation

a. Inciting violence or any other unlawful act against a woman or group of women by promoting misogynistic and violent attitudes or language based on gender, gender identity or expression, age, sexual orientation, race, ethnicity, religion, physical appearance, disability or any other vulnerability status;

b. Placing a woman or group of women deliberately in spaces of heightened visibility in order to facilitate attacks or to silence their opinions or complaints;

c. Blocking, disrupting, or deleting, individually or collectively, a woman's digital communication channels with the intent to restrict her participation or limit her expression in digital environments;

d. Harassing, intimidating, or defaming a woman through messages, comments, or degrading content motivated by gender;

e. Publishing, disseminating, and massively promoting false or malicious content and slander that harms a woman's image, reputation, or integrity.

Article 8. Manifestations of gender-based digital violence against women in public life, politics, or those actively participating in the digital environment

Manifestations of such violence include, among others:

a. Creating and/or disseminating harassing campaigns aimed at or resulting in the silencing, discrediting, disparaging, dehumanizing or demeaning of women in political or public spaces, including women's rights defenders and discourage their participation;
b. Sending digital messages that threaten or intimidate one or more women, their families, and/or individuals in their personal circle, with the aim or result of nullifying their political rights, including forcing their removal from seeking the office or resigning from the office or position they hold;
c. Disseminating, promoting, or amplifying, deliberately and in a coordinated manner, false or misleading content based on gender bias, stereotypes or misogyny, with the purpose or effect of discrediting, misinforming, intimidating, or censoring women in public or political life, or discouraging their participation in the digital environment;
d. Committing any other act legally defined as political gender-based violence against women that uses digital means to perpetrate it.

CHAPTER II
DUTIES OF THE STATE[9]

Article 9. Intersectional Approach and Differentiated Attention in the State Response

[9] The authorities entrusted with powers throughout Chapter II do not constitute an exhaustive or restrictive list. Each State, in adopting this Law, may assign or adapt such powers in accordance with its specific needs, institutional structures, and national context.

The relevant authorities responsible for the implementation of this law shall adopt measures to ensure that the prevention, protection, assistance, administration of justice, punishment, and reparation in cases of gender-based digital violence against women incorporate an intersectional perspective and differentiated attention approach. This approach shall address the diverse living conditions, identities, and contexts of women, including, among others, indigenous women, women of African descent, elderly and young women, migrants, women with disabilities, women residing in rural areas or in contexts of mobility, as well as any other condition or situation of vulnerability that increases their exposure to risk or limits their access to justice, protection, and full reparation for violations of their rights.

Article 10. Measures for the Prevention of Gender-Based Digital Violence Against Women

The authorities responsible for the implementation of this law include the governing bodies in charge of education, health, justice, human rights mechanisms, social services, digital technology and culture, including the comprehensive victim support system, in coordination with the National Mechanism for Women/Gender Affairs and other competent local authorities vested with legal authority. These entities shall:

a. Take all appropriate measures, including legislative measures, to amend or repeal existing laws and regulations or to modify legal or social and cultural patterns which sustain the persistence and tolerance of digital violence against women;
b. Undertake targeted actions to close the digital divide, with particular emphasis on women in vulnerable situations, using accessible formats and content adapted to diverse cultural contexts;
c. Promote equitable access for women to the digital environment, free from discrimination and violence, including affirmative actions to ensure the presence of women in the design and decision-making of digital technologies;
d. Provide specialized training on gender-based digital violence prevention policies to officials of the executive branch, justice system, electoral bodies, and political parties, as well as to personnel in the education and healthcare sectors, security forces, and all professionals handling violence against women, juvenile and child protection cases;
e. Develop and promote the use of digital technologies as tools for the empowerment of women, ensuring access to relevant information for the prevention, identification, and reporting of gender-based violence;
f. Establish and fund free, accessible, and culturally appropriate psychological, therapeutic, and mental health services for women victims of digital violence, as part of the comprehensive support system and in coordination with the health sector;
g. Develop temporary special measures as part of an emergency response system to address gender-based digital violence against women during national crises, such as a pandemic or a natural disaster.

Article 11. Educational, Psychosocial, and Comprehensive Training Measures for the Prevention of Gender-Based Digital Violence Against Women

National and local authorities with jurisdiction over education, health, childhood and adolescence, equality, culture, and technology, in coordination with the National Mechanism for Women/Gender Affairs and, where applicable, the comprehensive victim support system, shall design, implement, and strengthen public policies on education, psychosocial support, and resocialization that address gender-based digital violence against women in a comprehensive manner, in accordance with the following provisions:

a. Incorporate, in a cross-cutting and comprehensive manner at all levels of the formal education curriculum, content on digital literacy, digital citizenship, consent, self-care, digital, sexual, and reproductive rights, identification and response to online risks, and the prevention of gender-based digital violence, from a gender, human rights, and intersectional perspective;
b. Ensure ongoing, differentiated and specialized training for teaching, administrative, and management personnel in public and private educational institutions, for the proper detection, response, and referral of cases involving digital violence against women, including the adoption of institutional protocols to address gender-based digital violence;
c. Guarantee and strengthen the availability of psychosocial support mechanisms within educational, community, health, and child protection institutions, ensuring comprehensive assistance to women victims, as well as specialized intervention and support for perpetrators, particularly in cases involving children or adolescents, through trained interdisciplinary psychosocial teams;
d. Incorporate non-formal educational programs in community, parents' associations, cultural, sports, or recreational settings, particularly targeting at-risk populations, with content on the safe, ethical, and responsible use of digital technologies;
e. Implement resocialization measures with an educational and psychosocial focus for children and adolescents who have engaged in acts of gender-based digital violence, including mandatory participation in awareness programs, therapeutic support, supervised use of digital technologies, and restorative practices;
f. Promote active adult engagement with children and adolescents in navigating and participating in digital environments, through family and community education strategies aimed at fostering a culture of digital care;
g. Conduct awareness campaigns and formal and non-formal educational programs, disseminated through multiple platforms and accessible formats, aimed at dismantling gender stereotypes and preventing the normalization of digital violence.

Article 12. Measures To Prevent Gender-Based Digital Violence Against Women in Politics

Electoral administrative and judicial authorities, in cases involving gender-based digital violence against women politicians or electoral candidates, shall:

a. Promote training and educational initiatives, as well as instruments for the prevention of gender-based digital violence against women in politics within political parties, movements, alliances, coalitions, and intermediary organizations;
b. Ensure that electoral processes at all levels are conducted free from manifestations of gender-based digital violence against women in politics, including the

implementation of prevention and awareness-raising campaigns, monitoring observatories, risk assessments, and security plans aimed at protecting women engaged in political life, with particular emphasis on contexts of high polarization or prior threats;

c. Adopt a protocol establishing a summary and effective complaint procedure, the competent institutions for receiving and processing such complaints, and the mechanism for ordering protective and reparative precautionary measures, as well as the applicable sanctions in accordance with this law.

Article 13. Data and Statistics

For the purpose of monitoring the implementation and impact of this law, the National Mechanism for Women/Gender Affairs, along with the competent authorities and any other legally authorized entity on data and statistics, digital oversight, the judiciary, telecommunications, shall be responsible for generating and disseminating data and statistics. These entities shall:

a. Collect, systematize, analyze and publish data on gender-based digital violence against women;
b. Guarantee the traceability and accessibility of data and disaggregate it by age, gender, ethnicity, disability, economic status, territorial location, and other historically marginalized groups of women;
c. Adhere to ethical standards and safeguards for the protection of personal data and open data;
d. Assess the effectiveness of the measures adopted pursuant to this law and issue recommendations for their revision, where necessary;
e. Include both qualitative and quantitative indicators, process and outcome indicators, administrative records, and specialized surveys, as well as the inclusion of digital violence as a specific category within official statistical information systems on gender-based violence against women;
f. Ensure interoperability between entities responsible for collecting data and statistics and the justice system authorities.

Article 14. Inter-Institutional and Multi-Stakeholder Mechanism for the Prevention, Punishment and Eradication of Gender-Based Violence Digital Against Women

An interinstitutional and multi-stakeholder mechanism on Digital Governance shall be established, composed of representatives from the Executive and Judicial branches at all competent levels, political parties, the private sector, internet intermediaries, civil society, particularly women's organizations, afro-descendent and indigenous groups, women with disabilities and any other group historically marginalized or subject to vulnerability, as well as specialized academic institutions and experts in digital technology and cybersecurity. The primary functions of this body shall be to monitor and ensure accountability for the implementation of this law, guaranteeing the integration of a gender, human rights, and intersectional perspective in all its actions.

Competent institutions shall be required to submit periodic reports to this mechanism regarding their compliance with, and progress in, the implementation of this law.

The Mechanism shall have the authority to examine the reports of competent institutions, receive complaints and shadow reports regarding such institutions, investigate possible breaches by them, and make recommendations for the fulfillment of the obligations established under this Law.

Article 15. Measures for Comprehensive and Specialized Response

The competent bodies responsible for ensuring comprehensive and specialized response to women victims of gender-based digital violence include the Ombudsperson's Office, law enforcement authorities, the Ministry of Justice or the entity fulfilling that role, the National Mechanism for Women/Gender Affairs, and the governing entities on women's and gender issues at the various levels of the State, such as regional and provincial prosecutors' offices, and departmental and municipal secretariats for women and gender. These entities, in accordance with their constitutional, legal, and regulatory mandates, must:

a. Provide specialized services on digital violence and ensure that victims and practitioners receive comprehensive assistance grounded in a gender, human rights, and intersectional perspective, including psychosocial support, specialized physical and mental health care, and legal advice and representation, free of charge, and in an immediate, accessible, adequate, and priority-based manner, either virtually or in person;
b. Establish effective coordination mechanisms with specialized cybercrime prosecution offices and competent judicial authorities to ensure a coordinated and effective response;
c. Promote the development of specialized protocols for the response to cases of digital violence against women, incorporating a gender perspective and the use of appropriate technological tools and methodologies to identify and document patterns of systemic discrimination;
d. Define confidentiality standards for personnel responsible for handling cases of gender-based digital violence against women.

Article 16. Public Policy Measures for Protection

The National Mechanism for Women/Gender Affairs, the Judiciary, the Ministry of Justice, the Office of the Public Prosecutor, the Child and Adolescent Protection System, law enforcement authorities, and the regulatory body for Information and Communication Technologies, among other institutions legally vested with competence, shall coordinate the necessary actions to:

a. Ensure the comprehensive protection of victims by providing a timely and effective response at all stages of the proceedings, and by promoting coordination and collaboration among the various multisectoral actors involved;

b. Establish expedited reporting mechanisms, specialized protection procedures, and protocols for the collection and handling of digital evidence to enable a prompt and effective response;
c. Design a unified rapid response mechanism in coordination with digital platforms, aimed at facilitating cooperation between authorities and internet intermediaries in urgent cases of gender-based digital violence against women;
d. Promote periodic monitoring and evaluation processes for the protection and response measures adopted, to ensure their effectiveness and to enable evidence-based improvements;
e. Incorporate digital security services to protect victims' personal information, data, and accounts, as well as physical security measures in cases of serious threats, including police accompaniment and access to safe shelters or other appropriate forms of protection.

Article 17. International Cooperation

The State entities referenced in this law shall implement international cooperation strategies aimed at facilitating the achievement of the objectives of prevention, response, investigation, sanction, and reparation in cases of gender-based digital violence against women, recognizing its transnational nature.

Failure to implement such strategies may be understood as a form of tolerance or acquiescence by the State toward gender-based digital violence against women and may give rise to international responsibility for breach of the duty of due diligence in the context of transnational crimes.

This cooperation must be subject to clear safeguards ensuring the legality, necessity, and proportionality of the measures, as well as mechanisms for judicial review and oversight to prevent violations of the right to privacy or arbitrary use of such powers.

To that end, the State shall:

a. Enter into bilateral or multilateral agreements to establish joint investigative bodies for the crimes addressed by this law. In the absence of such agreements, joint investigations may be conducted through specific case-by-case arrangements, always respecting the sovereignty of the State in which the investigations are conducted;
b. Ensure mutual assistance through secure and expedited communication channels, including email, instant messaging, international calls, or other means that provide adequate levels of authentication and protection, including encryption where necessary;
c. Cooperate and assist in investigations and proceedings related to crimes of gender-based digital violence against women, including the collection and preservation of

electronic evidence, in accordance with applicable international instruments and mutual legal assistance treaties;

d. Facilitate, in urgent cases, the transmission of relevant information to another State when it may be useful for the conduct of investigations, proceedings, or judicial processes in the receiving State;
e. Apply measures such as preventive seizure, confiscation, forfeiture, and the transfer of evidence in electronic form, where applicable, provided that such measures comply with international human rights standards. These actions shall be carried out within judicial proceedings that guarantee the right to defense;
f. Promote the exchange of information on legislation, public policies, and good practices in this matter, including mechanisms for resolving jurisdictional conflicts;
g. Collaborate with internet intermediaries to trace and sanction aggressors. This cooperation shall be subject to the principles of legality, proportionality, and judicial oversight and shall not be used for the purpose of prosecuting individuals based on political opinion or personal characteristics.

In all cases, safeguards shall be included to allow the denial of international cooperation requests when there are well-founded reasons to believe that the request aims to prosecute, sanction, or discriminate against a person based on political opinion, gender identity, ethnicity, or other personal characteristics protected under human rights law.

CHAPTER III
THE REGULATION OF INTERNET INTERMEDIARIES FOR THE PURPOSES OF THIS LAW

Article 18. Co-regulatory Framework

This law will establish a co-regulatory framework for addressing gender-based digital violence against women, under which the State sets forth binding obligations and guiding principles, and internet intermediaries adopt their own mechanisms and policies for implementation, subject to the supervision and oversight of the competent authorities.

The co-regulatory framework will ensure the effective enforcement of this law through flexible and differentiated approaches that take into account the operational capacities of intermediaries, without prejudice to the full respect for human rights and the public order provisions established herein.

Internet intermediaries shall apply the principles of proportionality, necessity and legality and uphold procedural safeguards in their content moderation practices, establish mechanisms for risk assessment, due diligence, and procedures to address complaints related to the circulation of content not protected under the right to freedom of expression, and implement such processes diligently and in good faith.

The mechanisms adopted by intermediaries must be transparent, auditable, verifiable, and shall be designed in accordance with the principles of enhanced due diligence, gender perspective, intersectionality, necessity, legality, and proportionality. Such mechanisms must

also allow for periodic evaluation, ensure access to relevant information by competent authorities, and facilitate the meaningful participation of civil society in their review and ongoing improvement.

Article 19. Differentiated Regulatory Obligations for Large-Scale Internet Intermediaries

The obligations established in Articles 20, 21 and 25 of this law shall apply exclusively to internet intermediaries that:

a. Provide services to individuals located in or domiciled within the national territory;
b. Operate for profit;
c. Record an annual average of at least 100,000 users in the digital space;
d. Are classified as large-scale intermediaries and organizations in accordance with the national and/or regional regulatory framework.

The application of these provisions shall take effect regardless of the location of the intermediary's domicile or principal place of business. This differentiated application is intended to ensure regulatory proportionality, based on the intermediary's operational capacity, user volume, and social impact.

Article 20. Legal Representation of Internet Intermediaries

Internet intermediaries that offer their services within the territory, whether or not they have a physical establishment in the State, must designate in writing a natural or legal entity to act as their legal representative, vested with the necessary powers and sufficient resources to ensure effective and timely cooperation with the competent State authorities for the implementation of this Law.

The designated representatives shall be the recipients of communications from the competent authorities regarding all matters necessary for the receipt, compliance, and execution of decisions adopted in relation to this law.

Internet intermediaries must notify the full name, postal address, contact information, email address, and telephone number of their legal representative to the Ministry or Secretariat of Commerce, the National Mechanism for Women/Gender Affairs, the Ministry or Secretariat with competence in Information and Communications Technologies, and any judicial or regulatory authority overseeing economic activity, as applicable.

Article 21. Points of Contact

Internet intermediaries must designate specific points of contact for both the competent State authorities and users to ensure effective communication for the implementation of this Law. The relevant contact information must be made public, clearly presented, accessible, and easily identifiable on the intermediary's official platforms or communication channels.

The designated points of contact must provide communication options that are not limited to the exclusive use of automated tools, and must guarantee mechanisms that enable direct, prompt, and simple access to human representatives of the intermediary.

Article 22. General Terms and Conditions

Internet intermediaries must provide a clear, accessible, and detailed description of the general terms and conditions applicable to the use of information provided by users, as well as any restrictions associated with the use of their services. This information shall include, at a minimum: privacy policies concerning the processing of personal data; the procedures, measures, and tools used for content moderation and curation, including the use of automated algorithms and impartial human review mechanisms; and the internal rules and protocols governing the handling of complaints and reports, ensuring a timely, objective, and transparent response.

Intermediaries must also inform users of any significant changes to the general terms of service, ensuring that such communication is clear, timely, accessible and easily understandable.

Article 23. Internal Policies for the Prevention of Gender-Based Digital Violence Against Women

Internet intermediaries shall adopt comprehensive internal policies to prevent gender-based digital violence against women, incorporating effective mechanisms for detection, response, and accountability. To comply with these obligations, they must:

a. Implement preventive measures aimed at timely identification and response to incidents of digital violence;
b. Establish accessible and effective procedures for complaints and appeals regarding content moderation and curation decisions, consistent with the rights recognized under this law and aligned with principles of international human rights law;
c. Provide information related to the use of their services, general terms and conditions, users' rights, and protection mechanisms in clear, simple, comprehensible, and accessible language, using formats compatible with various electronic devices.
d. Promote the equitable participation of women in the design and implementation of digital technologies to combat algorithmic bias.

Article 24. Moderation of Content

Internet intermediaries must implement effective content moderation systems to prevent and halt the reproduction or conceal materials that constitute manifestations of gender-based digital violence against women, as provided in Articles 2, 7, and 8 of this law, while ensuring the preservation of evidentiary material. They must also ensure systematic and up-to-date training in gender perspective, women's human rights, and intersectionality for personnel responsible for moderation.

Moderation must be conducted through the following three primary mechanisms:

a. User complaints, submitted through accessible and efficient systems that allow individuals to report content constituting gender-based digital violence against women;
b. Government requests, issued by competent authorities through precautionary measures for the removal or restriction of content and/or by judicial order, issued by a competent judicial authority in accordance with due process guarantees;
c. Automated tagging, through algorithms designed to detect content that may constitute gender-based digital violence against women, in accordance with Articles 2, 7 and 8 of this Law. Where automated tagging identifies a potential manifestation of such violence, the case shall be subject to review by an impartial internal evaluation team with specialized expertise in human rights and gender-based violence, as mentioned in Article 25 of this law.

All decisions adopted in the context of content moderation may be subject to subsequent judicial review in order to ensure compliance with international principles of legality, necessity, and proportionality, as well as full respect for due process and international human rights law. The procedures under this article shall be conducted in an open, verifiable, diligent, objective, and proportionate manner, with due consideration for the rights and legitimate interests of all parties involved, in coordination with State authorities.

Article 25. Internal Evaluation Team

Internet intermediaries must establish an internal evaluation team composed of qualified and specialized human personnel within the local context, and shall also include representatives of civil society and independent bodies with expertise in human rights and technology. The composition of this team shall ensure an appropriate balance between the protection of women's rights and the safeguarding of freedom of expression and access to information in the digital environment.

This team shall be responsible for analyzing user reports, complaints, and appeals, content identified through systemic risk assessment mechanisms arising from the intermediary's operations, and cases flagged through automated tagging, where algorithms are designed to identify possible manifestations of gender-based digital violence against women in accordance with this law.

Article 25 bis. Functions

The team shall adopt the most appropriate measures to ensure effective protection of women's rights in digital spaces. These measures may include, among others: content removal, temporary or partial suspension of services for the responsible party, implementation of educational initiatives, or any other necessary action to prevent harm and ensure compliance with the provisions of this law.

The team shall conduct a comprehensive evaluation of the risks associated with the continued availability of the content, taking into account not only its nature but also its potential to exacerbate harm. This shall include consideration of factors such as the impact generated,

including the volume of content shared, the speed of its dissemination, its reach, and the persistence of the material on systems or servers.

The outcomes of the evaluation process must be easy for users to understand, find, and use, and must be accessible, effective, and provide timely responses, ensuring accountability, support for victims, and respect for human rights.

Article 26. Measures for Moderation of Content or Services

The internal evaluation team may adopt measures to suspend, restrict, or remove content or services when it determines the existence of manifestations of gender-based digital violence against women, in accordance with Articles 2, 7, and 8 of this law.

Sanctions must be applied progressively and proportionately to the severity of the incident, including, but not limited to:

a. Temporary and progressive suspension of access to or provision of specific services, depending on the level of risk or recurrence;
b. Deactivation of monetization features or promotion functions for content identified as gender-based digital violence;
c. Voluntary removal of unlawful content or harmful content in cases involving girls and adolescents, to prevent revictimization and safeguard their comprehensive development;
d. Adoption of non-criminal measures for reparation of harm, such as symbolic compensation, measures of satisfaction, or guarantees of non-repetition;
e. Public retraction, when appropriate, as a mechanism for acknowledging the harm caused and accepting responsibility before the affected community.

These sanctions shall be applied without prejudice to any other criminal, civil, or administrative liabilities established under applicable law.

In cases involving material depicting sexual violence or exploitation of girls or adolescents, the associated account shall be immediately suspended, and any unlawful content, or harmful content in cases involving girls or adolescents, must be promptly removed, without prejudice to the referral of the case to the competent authorities.

Article 27. Definitive Measures for Moderation of Content or Services

In cases where it is determined that an unlawful act has been effectively and concretely committed, with the potential to cause harm to the rights of one or more women, and in accordance with Articles 2, 7, and 8 of this Law, the internal evaluation team shall, on an exceptional basis, adopt definitive suspension or removal measures. These may include but are not limited to the deletion or blocking of misogynistic content, suspension or restriction of payments, disabling of monetization functions, full interruption of service, or suspension or termination of user accounts.

In all cases, users must be guaranteed the right to appeal decisions. Users may first request a review before the internal evaluation team and subsequently seek reconsideration by an

external and independent committee. These mechanisms shall ensure compliance with due process guarantees, decision-making transparency, and accountability on the part of the intermediary.

All measures adopted must be communicated through a clear and specific statement of reasons, enabling users to understand the basis for the decision. Additionally, all relevant data and digital records, such as content, traffic data, connection logs, and metadata associated with the account, must be preserved to ensure their availability in the event of judicial proceedings or requests by competent authorities.

Persons affected by these measures may challenge their legality through judicial proceedings, including the compatibility of the measure with the right to freedom of expression, and may request their reconsideration, continuation, or revocation as appropriate.

Article 28. Internal Complaint Mechanisms

Internet intermediaries must implement accessible and effective internal complaint mechanisms that enable users to report content that violates the rights protected under this law and to request its removal, suspension, or restriction. Such mechanisms shall ensure the preservation of evidentiary material, including any related digital data and user information, for potential use by the competent investigative authorities.

These mechanisms must be easy to understand, readily identifiable and usable by users, accessible at no cost, and shall guarantee a prompt, timely, and justified/reasoned response. Their operation shall adhere to principles of transparency, due diligence, proportionality, legality, and necessity. All complaints must be assessed by the internal evaluation team in a non-discriminatory, diligent manner, consistent with the principles of this law and international human rights standards.

Intermediaries shall also be required to ensure accountability and provide users with clear and accessible information regarding the reported or identified content, the status of the procedure, and the decision rendered, including the justification for such decision, in accordance with the principles of transparency and institutional responsibility.

Article 29. Internal Appeal Mechanisms

Internet intermediaries must establish effective internal appeal mechanisms that enable users to challenge any decision involving the removal, restriction, suspension, or any other measure taken in relation to their content, accounts, or access to services.

Such mechanisms must be accessible, free of charge, prominently displayed, and easy to understand and use. They shall be designed to ensure that users can submit complaints in a straightforward manner where they believe that the actions taken are unjust or infringe upon their rights.

Decisions rendered through the appeal process must be issued promptly, be duly reasoned, non-discriminatory, and comply with the principles established under this law and with applicable international human rights standards.

Where an appeal is upheld, the internet intermediary shall promptly correct or reverse the measure taken, without delay.

Article 30. Compliance with Requests from Competent Authorities

When the designated point of contact for State authorities or the legal representative of the internet intermediary receives an order issued by a competent national judicial and/or administrative authority, whether to take action concerning one or more instances of content within the scope of this law, or to provide specific information related to one or more users, the intermediary must:

a. Verify that the order or request originates from an authority duly empowered under the applicable national legislation, and that it is properly substantiated and reasoned, in accordance with the principles of legality, necessity, and proportionality;
b. Act without delay to fulfill the request, giving immediate effect to the measures required by the issuing authority;
c. Provide written notification to the issuing authority, or to any other authority expressly designated therein, detailing the actions undertaken and the dates on which such actions were executed;
d. Maintain detailed documentation of the procedure followed, including the date and time of receipt of the order, the identity of the issuing official, the actions taken, the individuals responsible for implementation, and the response timelines;
e. Retain a complete copy of the order and related case file for a minimum period of five (5) years, for purposes of audit, institutional accountability, or legal defense;
f. Periodically compile and publish disaggregated statistical reports with a gender analysis indicating the number and types of orders and requests received, the issuing authorities, and the compliance rate, for the purpose of promoting transparency and institutional accountability.

The processing of personal data in connection with these procedures must strictly comply with applicable data protection and confidentiality regulations, and shall ensure the prevention of misuse, unauthorized access, or re-victimization.

Where the request originates from an administrative authority, the corresponding action may be subject to subsequent judicial review to ensure conformity with the international principles of legality, necessity, and proportionality, as well as full respect for due process and international human rights law.

Article 31. Content Curation with a Gender Perspective

Internet intermediaries engaged in content curation activities must ensure that the criteria used to select, organize, and present information, data, or digital content do not perpetuate gender stereotypes or reinforce discriminatory biases that disproportionately affect women.

Content curation practices must incorporate safeguards to prevent recommendation, search, or prioritization systems from increasing exposure to content constituting gender-based digital violence against women, including misogynistic speech, gendered disinformation, silencing practices, and harmful content in cases involving girls and adolescents.

To ensure transparency and accountability in content curation processes, intermediaries must:

a. Provide and publish clear, accessible, and understandable information regarding the general criteria used in content curation, including whether such criteria are based on commercial interests, automated algorithms, or editorial decisions;
b. Enable users to access and configure their content display and personalization preferences, including options to limit or exclude content that may be harmful or discriminatory;
c. Conduct regular internal or independent audits to identify adverse impacts arising from content curation on the exercise of women's rights, and adopt corrective measures where gender bias or disproportionate effects are detected;
d. Incorporate a gender, human rights, and intersectional perspective in the design, review, and update of recommendation and content presentation systems.

Under no circumstances shall content curation practices result in indirect discrimination or unjustifiably restrict women's access to information, public participation, or the full exercise of their rights in the digital environment.

Article 32. Algorithmic Accountability

Internet intermediaries that utilize algorithms in the provision of their services must design, implement, and manage such systems in a transparent, ethical, and accessible manner, ensuring that they are understandable in local languages and culturally appropriate, particularly for groups in situations of vulnerability.

Intermediaries must make available to users clear, comprehensible, and easily accessible terms of service, enabling them to make informed decisions regarding the use of such services and to provide or withdraw their consent freely, deliberately, and at any time.

Intermediaries must establish effective mechanisms to ensure that users retain full control over their digital experience, including the ability to customize functionalities, limit interactions, modify algorithmic preferences, and manage their exposure to content in accordance with their own criteria.

Algorithms employed by internet intermediaries must incorporate safeguards aimed at preventing gender-based digital violence against women. In particular, such systems shall be designed to avoid the amplification of unlawful content or harmful content in cases involving girls and adolescents, or content that infringes upon women's rights. Algorithms shall also be free from bias and stereotypes that perpetuate violence or discrimination. Their design shall contribute to the creation of a safe, respectful, and human rights–protective digital environment.

Article 33. Duty to Respect Human Rights

Internet intermediaries must apply the principle of safety by design and by default, ensuring the protection of users' human rights by incorporating effective safeguards from the inception of any new technology, tool, or functionality offered through their services, in order to

prevent misuse or malicious use, particularly in contexts of gender-based violence against women.

Intermediaries must also be required to carry out, at their own expense and at least once per year, independent audits to assess their compliance with the provisions of this law. The resulting audit reports shall be published in accessible formats and in accordance with the principle of explainability. These reports must include, at a minimum: internal statistics on cases identified as gender-based digital violence against women; the preventive, corrective, and improvement measures implemented; and the outcomes achieved, thereby ensuring transparency and accountability in their practices.

Based on the findings of these independent audits, and in coordination with competent State authorities, intermediaries shall continuously develop and implement digital literacy, education, and awareness-raising campaigns, tailored to local contexts, with the aim of promoting women's human rights and strengthening their capacities in digital security.

CHAPTER IV
JUDICIAL PROCEEDINGS

I. GENERAL PRINCIPLES OF THE PROCEEDINGS

Article 34. Guiding Principles of the Proceedings

Actions related to the investigation and prosecution of gender-based digital violence against women shall be governed by the following principles:

a. Due diligence, independence, impartiality, and appropriateness;
b. Gender perspective, intersectionality, equality, non-discrimination and victim-centered approach, and trauma sensitivity;
c. Guarantee of sufficient technical, human, and financial resources;
d. Personnel trained in digital violence against women and in techniques for collecting and preserving digital evidence;
e. Evidentiary standards free from gender stereotypes, biases, and prejudices, ensuring credibility and fair treatment of victims;
f. Due process;
g. Cultural relevance;
h. Guarantee of privacy in the handling of personal data;
i. Principles of legality, proportionality, necessity, and adequacy;
j. Subsequent liability for any restriction on freedom of expression;
k. Prohibition of prior censorship and the use of precautionary measures implying content blocking without a justified judicial order.

Article 35. Rights of Victims/Survivors in Proceedings

The competent national mechanisms, such as the Ministry of Justice, the Office of the Public Prosecutor, the Judiciary, among others, shall guarantee the following rights to women victims and survivors, as well as their family members, through the creation of specific guidelines:

a. Access justice, including free and specialized legal representation throughout the national territory, specialized psychological assistance, and comprehensive support measures during judicial proceedings;
b. Be informed of their rights, to have their opinions, needs, interests, and concerns heard by the investigative authority and the courts, and to fully participate in all stages of the process;
c. Have their privacy guaranteed and to be protected from revictimization or retraumatization;
d. Receive reasonable accommodations that enable effective access to justice, particularly for women in situations of vulnerability, including women with disabilities, pregnant, young, or elderly; women belonging to racial, ethnic, migrant, refugee, or displaced groups; and those in socioeconomically disadvantaged situations or affected by armed conflict or deprivation of liberty;
e. Be provided with a translator and/or interpreter according to their nationality, language, dialect, disability, race or ethnic origin, or condition as migrant, refugee, or displaced person;
f. Ensure that foreign and migrant women, as well as their dependents, are not deported as a consequence of filing a complaint, even if they are in an irregular migration situation.

In cases where the justice system employs digital tools, such as artificial intelligence, human oversight and review shall always be ensured to prevent algorithmic biases that may infringe upon the rights of women recognized under this Law[10].

Article 36. Jurisdiction

The competent courts, in accordance with the Constitution and the laws of the State, shall have jurisdiction over the offences established under this Law in the following cases:

a. When the offence is committed wholly or partially within the national territory;
b. When the victim is a woman who is a national, resident, visitor or migrant of the State;
c. When the perpetrator is a citizen or resident of the State;
d. When the services related to the offence are accessed from the national territory, irrespective of the principal place of business or domicile of the internet intermediary.

Article 37. Child or Adolescent Offender

For the purposes of this law, a child or adolescent offender is any person under eighteen (18) years of age who is responsible for acts of gender-based digital violence against women, as defined by this law and within the framework of the comprehensive protection system for the rights of children and adolescents.

---

[10] *See* United Nations. (2025). *Artificial intelligence in judicial systems: Promises and pitfalls* (Report of the Special Rapporteur on the independence of judges and lawyers, A/80/169).https://www.ohchr.org/en/documents/thematic-reports/a80169-ai-judicial-systems-promises-and-pitfalls-report-special

Recognition of a child or adolescent as the perpetrator of such acts does not entail automatic equivalence with adult criminal liability. Their treatment must be governed by the principles of specialization, the best interests of the child, proportionality, non-discrimination, educational opportunity, and differentiated responsibility, in accordance with specialized legislation on childhood and adolescence.

Applied measures shall prioritize restorative, socio-educational, and comprehensive protection approaches, aimed at fostering awareness of the harm caused, promoting symbolic or effective reparation, preventing recidivism, and contributing to the transformation of behavioral patterns that perpetuate violence and gender inequality, without prejudice to the victim's rights or the procedural guarantees of the child or adolescent involved.

Article 38. Legal Standing

A complaint may be filed by the victim or survivor, by third parties or any natural or legal entity, or ex officio by competent authorities, provided the case involves a public-action offence of gender-based digital violence against women. In the case of private-action offences of gender-based digital violence against women, the complaint may only be filed with the express authorization of the victim.

II. PRECAUTIONARY MEASURES AND PRELIMINARY INJUNCTIONS

Article 39. Competent Authorities Responsible for the Receipt of Complaints of Gender-Based Digital Violence Against Women

Complaints regarding manifestations of gender-based digital violence against women may be submitted, either orally or in writing, with or without legal counsel, before any of the following authorities:

a. The Public Prosecutor's Office or the Attorney General's Office;
b. Police stations or precincts;
c. The Special Gender-Based Violence Units;
d. The Division for the Protection of Children, Adolescents, Women and Family within the competent investigative body with relevant jurisdiction;
e. Law enforcement agencies;
f. The electoral authorities;
g. Border control units;
h. Any Competent Courts or Judicial Authorities;
i. Any agency or entity within the country established to monitor cyber-crime;
j. Any other entity expressly granted such competence.

Authorities receiving such complaints may order urgent precautionary measures in cases of emergency or imminent harm, in accordance with the principles of legality, necessity, proportionality, and comprehensive protection of the rights of the victim.

Article 40. Precautionary Measures and Preliminary Injunctions

Precautionary measures and preliminary injunctions, described in Article 41, must be applied to prevent irreparable harm to the rights of the victim or to ensure the preservation of evidentiary material, and must be subject to immediate judicial review. Their adoption shall adhere to the principles of legality, necessity, and proportionality, and shall comply at all times with international human rights standards.

a. Precautionary measures shall refer to those adopted before the initiation of a formal judicial or administrative process, where there is evidence of imminent harm to the victim's integrity or risk of loss or tampering with evidence. Authorities competent to receive complaints, as set forth in Article 39 of this law, may adopt urgent precautionary measures or request their issuance by the competent judicial or administrative authority.

b. Preliminary injunctions are those issued during judicial proceedings. The competent Court may impose such measures at the request of the Public Prosecutor's Office, the victim, her legal representative, or any other competent authority as provided in Article 39 of this law. Where a request for a preliminary injunction is submitted within the legally prescribed period, the matter shall be decided without delay upon the filing of the complaint.

Article 41. Types of Precautionary Measures and Preliminary Injunctions

The competent administrative or judicial authority may order, through a duly reasoned decision, one or more of the following measures, either urgently prior to the initiation of a formal proceeding as precautionary measures, or within the framework of judicial proceedings as preliminary injunctions, to protect the victim, preserve evidence, and ensure the proper course of the procedure:

a. Prohibit the alleged aggressor from physically approaching the victim or communicating with her by any means, including digital channels. Such prohibition shall extend to persons under the care or protection of the victim;
b. Order the temporary and controlled removal of digital content that may constitute gender-based digital violence against women, ensuring the preservation of such material as evidence in accordance with established protocols;
c. Restrict profiles, access, functionalities, or digital interactions that pose a risk to the victim's rights;
d. Order any other measure necessary to prevent irreparable harm, avoid revictimization, or safeguard the victim's integrity.

Any measure involving the blocking or restriction of fundamental rights must be authorized and/or subject to review by a competent judicial authority, in accordance with the principles of legality, necessity, proportionality, and subsequent liability.

Article 42. Procedure for the Adoption of Precautionary Measures and Preliminary Injunctions

Criminal, civil, administrative, electoral courts, as well as courts vested with specialized jurisdiction over matters concerning children, adolescents, and gender-based violence, shall have jurisdiction over the imposition, review, challenge, and enforcement of precautionary measures, as well as the issuance, review, and suspension of preliminary injunctions under this law.

All decisions shall be duly reasoned and formally notified to the parties concerned.

III. CRIMINAL LIABILITY

Article 43. Criminal Offences

The actions described in subsections *a* through *d* of Article 7.1. of this Law shall be classified as public-action offences. The foregoing shall not be understood as an exhaustive or limiting list.

Article 44. Penalties

Criminal offences established under this Law shall be punishable by imprisonment and/or other measures as may be necessary to ensure the protection of victims or survivors of gender-based digital violence against women, including fines or equivalent sanctions. In no case shall the penalty imposed be less severe than that prescribed under national law for comparable offences.

The victim shall, in all cases, have the right to bring a civil action for damages before the competent courts, either independently or in addition to the criminal proceedings.

Article 45. Aggravating Circumstances

The following shall be considered aggravating circumstances in the commission of gender-based digital violence against women:

a. That the offence was committed against a person in a situation of vulnerability, whether due to conditions of dependency, physical, mental, intellectual, or sensory disability; being a child or adolescent; or based on the person's sexual orientation, gender identity or expression, religion, social origin, political beliefs, ethnic-racial background, or other circumstances that increase exposure to risk or hinder access to protection and justice;
b. That the offence was perpetrated by two or more persons acting jointly;
c. That the offence was preceded or accompanied by acts of physical, psychological, emotional, economic, or sexual violence or abuse, or committed through the use of force, coercion, or threats, whether or not involving the use of a weapon;
d. That the offence was committed with premeditation, planning, or prior deliberation, demonstrating the intent to cause aggravated, prolonged, or irreparable harm to the victim or survivor;

e. That the criminal conduct resulted in the death of the victim, caused serious physical or psychological injury, or led the victim or survivor to attempt against their own integrity as a consequence of the effects or impacts of the offence;
f. That the offence was perpetrated against a spouse, former spouse, actual, former or perceived intimate or sexual partner of any duration, a member of the victim or survivor's family by blood or affinity, or a person with whom they had or have an emotional, affective, or trust-based relationship;
g. That the offence was committed through abuse of a position of authority or influence over the victim or survivor;
h. That the perpetrator had been granted access to documents, photographs, correspondence or other sensitive materials owned by the victim or other person in the performance of a service, such as maintenance of devices or files that were used to carry out or facilitate the offensive conduct.

Article 46. Institutional Responsibility in Investigation and Punishment

The Public Prosecutor's Office or the Attorney General's Office, the Judiciary in all its branches, security forces, and administrative bodies with regulatory and sanctioning authority shall be responsible for:

a. Initiating appropriate proceedings for public-action offences;
b. Prosecuting, investigating, and imposing criminal, civil, and administrative sanctions for acts of digital violence as provided under this Law;
c. Ensuring access to justice, truth, and reparation for women victims and their families, acting with due diligence;
d. Ongoing and differentiated strengthening capacity-building of personnel on gender-based digital violence against women, including the latest techniques for preserving digital evidence;
e. Preserving evidentiary material and ensuring its integrity.

Article 47. Guarantees in the Investigation and Punishment Process

Procedures related to the investigation and punishment of gender-based digital violence against women shall respect the following principles:

a. Serious, impartial, and effective action with a human rights, gender, intersectional, equality, and non-discrimination approach;
b. Application of the principle of subsequent liability for any restriction on freedom of expression;
c. Prohibition of prior censorship and the use of preliminary injunctions that entail blocking content without a substantiated judicial order;
d. Application of the principles of necessity, legality, suitability, and proportionality for the restriction of content in all cases.

Article 48. Institutional Coordination and Specialization

Specialized units or teams shall be created or strengthened for the investigation and punishment of gender-based digital violence against women, equipped with trained

personnel, technological tools, and adequate budgetary resources to effectively carry out their duties.

In addition, permanent inter-institutional coordination mechanisms shall be established with cybercrime prosecutors' offices, competent judicial bodies, and internet intermediaries, to ensure a timely, coordinated, and human rights-based response to this form of violence.

Article 49. Obstruction of Access to Justice

Any person who hinders or obstructs protective measures, the investigation, prosecution, or punishment of offences of gender-based digital violence against women shall be subject to the penalty established for the crime of obstruction of justice under national law. Where the perpetrator is a public official acting in the exercise of or in connection with their duties, such person shall be sanctioned with the penalty corresponding to the crime of obstruction of justice, as well as disqualification from holding public office.

Article 50. Elimination of Exonerating or Mitigating Grounds

Exonerating or mitigating grounds that promote or justify gender-based violence against women, such as violent emotion, anger, provocation by the victim, honor, jealousy, cultural beliefs, customs contrary to human rights, extreme distress, or similar arguments, shall not constitute exonerating or mitigating circumstances for criminal liability in cases of gender-based digital violence against women.

IV. ADMINISTRATIVE, CIVIL, AND ELECTORAL LIABILITY

Article 51. Administrative Infractions

The actions described in Article 7, subsections 7.1.h, 7.2.a, 7.3.b, and 7.3.c. of this law shall constitute grounds for administrative liability for public officials who engage in such acts, in accordance with the provisions of this law.

In such cases, the victim may also initiate a corresponding civil action before the competent jurisdiction to obtain reparation for the damages arising from such conduct.

Article 52. Liability of Public Officials

Public officials shall incur civil, criminal, and administrative liability, in accordance with the harm caused, whether by act or omission, when, having direct or indirect knowledge of facts that could constitute gender-based digital violence against women, and being legally obliged to act by virtue of their office or duties, they fail to do so, obstruct the institutional response, promote impunity, or, through inaction, allow the harm to persist or new risks to arise concerning the rights of victims.

Such liability shall extend to situations where:

a. Knowledge of the facts arises from formal or informal sources, including monitoring systems, institutional alerts, or reasonable evidence, and is not limited solely to complaints filed by the victim;
b. Unnecessary duplication of procedures or actions by different entities occurs, leading to secondary victimization;
c. The duty to provide comprehensive protection in accordance with the standard of enhanced due diligence in addressing gender-based digital violence against women with an intersectional approach is not fulfilled;
d. Adequate legal representation is not provided for women, especially girls, adolescents, with disabilities, indigenous, marginalized or in other forms of vulnerability;
e. Confidentiality rules are breached by personnel responsible for handling cases, thereby incurring liability for the improper, negligent, or wrongful handling of information related to victims.

Article 53. Administrative Liability of Internet Intermediaries

Internet intermediaries shall incur administrative liability before the competent Courts in the following circumstances:

a. When they engage in one or more of the forms of gender-based digital violence against women as defined in Article 7 of this law;
b. When they have failed to adopt reasonable measures to prevent one or more of the forms of gender-based digital violence against women as set forth in Articles 43 and 58 of this law, when such acts are committed by: (i) their employees, (ii) contractors, (iii) managers, or (iv) associates, whether belonging to the intermediary itself or any affiliated legal entity;
c. When, notwithstanding the cessation of the harmful conduct referred to in Article 7 of this law, there are sufficient grounds to indicate that such conduct is likely to recur imminently, and no appropriate measures have been adopted to prevent its repetition;
d. When they fail to act upon notification of unlawful content or harmful content in cases involving girls and adolescents, made available through the services they provide, or when they do so without justification or in bad faith, thereby infringing their rights protected under this Law.

Article 54. Administrative Procedure before the Competent Courts

The procedure before the Competent Courts applicable to internet intermediaries shall guarantee their right to be notified of the charges brought against them, to exercise their right of defense, to submit relevant arguments and evidence, to be heard under conditions of equality, and to file the appropriate appeals against any decision rendered, in accordance with the provisions of this Law and the applicable national procedural legislation.

Before issuing a final decision, the Competent Court shall formally notify the intermediary, in advance, of the preliminary conclusions of the case.

Such notification shall include, at a minimum, the following:

a. The identified violations or breaches;
b. The corrective measures the intermediary is expected to adopt in order to remedy the breach;
c. A reasonable period, as determined by the Court, within which the intermediary may submit observations, provide evidence, or implement immediate corrective measures.

Upon expiry of the granted period, if the intermediary sufficiently demonstrates that it has adopted the required measures and remedied the breach, the Court may conclude the proceedings, recording its reasoned decision.

If, on the contrary, the intermediary fails to adopt the required measures within the established period, or if such measures are deemed insufficient, the competent Court shall proceed with the case and impose the corresponding sanctions, in accordance with the provisions of this Law and the applicable national procedural legislation.

Article 55. Administrative Sanctions for Internet Intermediaries

The competent Courts shall impose one or more of the following sanctions on internet intermediaries found to have committed any of the acts described in Article 53 of this law:

a. Monetary fines proportional to the severity of the infringement, up to six percent (6%) of the intermediary's global annual revenue for the preceding fiscal year. The court may order that a portion of the fine be allocated to the implementation or enhancement of programs addressing the eradication of gender-based digital violence against women;
b. Prohibition from receiving any form of government incentives or subsidies for a period proportionate to the harm caused;
c. Revocation of the authorization to operate within the national territory, either temporarily or permanently, in cases of serious or repeated violations.

Article 56. Allocation of Resources Derived from Economic Sanctions

The funds collected from economic sanctions imposed through administrative proceedings for acts of gender-based digital violence against women shall be allocated as a priority to the comprehensive support of victims, as well as to the strengthening of institutional capacities and the technological infrastructure necessary to ensure the effective implementation of this law within the State.

Article 57. Civil Infractions

The actions described in Article 7, subsections 7.1.f, 7.1.g., 7.2.b, 7.2.c, 7.2.d, 7.3.d, and 7.3.e of this law shall constitute civil infractions and give rise to liability in accordance with the

applicable legal provisions, without prejudice to the imposition of additional sanctions where appropriate. This list shall not be interpreted as comprehensive or exclusive.

Such actions may also constitute criminal offences when committed in a persistent, repeated, and deliberate manner, and where it results in serious harm to the physical, psychological, or sexual integrity, or to the liberty of the victim, in accordance with the applicable criminal classification and with full respect for due process guarantees.

Where the perpetrator is a minor, the special liability regime established under the legislation on children and adolescents shall apply, without prejudice to the victim's right to obtain appropriate reparation, which may be enforced through the joint liability mechanisms provided under applicable law, including the joint liability of those charged with the minor's care or guardianship.

Article 58. Concurrent Criminal, Civil, and Administrative Liability

The actions described in Article 7, subsections 7.1.i and 7.3.a of this law could constitute unlawful acts that may give rise to criminal, civil, and administrative liability. These forms of liability may be pursued concurrently, in accordance with the nature and gravity of the acts, and as provided under this law and the applicable legal framework.

Article 59. Liability of Legal Entities

Legal entities shall be subject to civil and/or administrative liability for their direct or indirect involvement in the commission of acts classified as criminal offences under article 43 of this Law, without prejudice to the individual criminal liability of the natural persons responsible for their execution.

The liability of legal entities shall be applicable in the following cases:

a. Where the unlawful act was committed, in the name of or on behalf of the legal entity, by any person exercising functions of direction, administration, representation, or control within the organization, acting within the scope of such functions;
b. Where the unlawful act was committed by a natural person acting under the authority or instructions of a person exercising managerial or representative functions, provided that the act was enabled by the failure to exercise proper control or supervision.

Article 60. Civil Liability of Internet Intermediaries

Internet intermediaries shall incur civil liability for damages caused when, by act or omission, they engage in one or more of the manifestations of gender-based digital violence against women set forth in Articles 7 and 8 of this law, or when they have facilitated, tolerated, or failed to reasonably prevent the commission of such acts, in accordance with their role, duties, and technical capabilities.

In proceedings for civil liability, the competent Courts shall have the authority to evaluate conduct that, in the context of providing digital services, has the purpose or effect of

committing gender-based digital violence against women, whether such conduct is attributable to natural or legal entities.

Victims may seek civil liability for acts which, even if not criminally classified, constitute a violation of their rights, particularly those recognized in Articles 53, 57, and 58 of this law, as well as under the Belém do Pará Convention and other international human rights instruments ratified by the State.

Civil actions may be brought independently or jointly with other judicial proceedings, whether criminal or administrative, and shall entail the obligation to provide full reparation for both material and moral (non-material) damages in accordance with the Civil Code and the Code of Civil Procedure.

Article 61. Electoral Offences and Infractions

Conducts described in article 8 of this law, when committed in the context of political or electoral processes, shall constitute infractions or offences punishable in accordance with applicable electoral law and the provisions of this Law.

The competent electoral jurisdictional body, or, where the electoral body does not have this authority, the Court, may impose, as appropriate, sanctions such as public or private admonitions, suspension from public office or duties, suspension of salary, imposition of fines, and the immediate removal of messages or content that contravene the provisions of this Law.

Fines or other sanctions may be imposed on political parties, candidates, electoral alliances, or organizations that directly or indirectly participate in organized attacks against women in political spaces or in any other manifestation of gender-based digital violence covered under this law, but not described in Article 8.

These sanctions shall also apply to any individual who engages in gender-based digital violence against women in the political or electoral sphere, including candidates, political party representatives, public officials, and other actors involved in such processes.

V. REPARATION AND GUARANTEES OF NON-REPETITION

Article 62. Reparation and Guarantees of Non-Repetition Measures in Cases of Gender-Based Digital Violence Against Women

Women victims of gender-based digital violence have the right to comprehensive, adequate, effective, transformative reparation, incorporating a gender, human rights, and intersectional perspective. Such reparation must acknowledge the magnitude of the harm suffered, restore violated rights, and contribute to the eradication of the structural causes of violence. Effective, free, and accessible criminal, civil, and administrative judicial mechanisms shall be guaranteed to make the right to comprehensive reparation enforceable, along with the creation of specific funds to ensure the implementation of such measures, including when the perpetrator lacks the capacity to comply with them or cannot be individually identified.

Comprehensive and transformative reparation shall include, in a complementary and non-exhaustive manner, the following measures:

a. Actions aimed at restoring the situation prior to the manifestation of violence, including, where possible, the removal of unlawful content, the restoration of digital identity, and the reparation of harm caused to the victim's honor and reputation;
b. Financial compensation proportionate to the material and non-material harm caused, including, among others, loss of income, psychological harm, medical and legal expenses;
c. Free and appropriate access to social services that contribute to the comprehensive recovery of direct and indirect victims and the reconstruction of their life plans;
d. Public acknowledgment of the harm caused, as well as institutional or perpetrator-issued apologies where appropriate;
e. Symbolic reparation measures, guarantees of truth and justice, and other efforts to dignify the victim;
f. Institutional, legislative, educational, and technological reforms that ensure the non-repetition of similar acts.

Such measures shall be designed and implemented with the active participation and informed consent of the victims, ensuring their safety, dignity, privacy, and identity, and applying an intersectional and differentiated approach in the case of girls, adolescents, indigenous women, Afro-descendant women, women with disabilities, LBTI women, migrant women, or women in other situations of vulnerability.

Article 62 bis. Reparation Measures and Guarantees of Non-Repetition for Internet Intermediaries

The competent Courts and authorities, in accordance with the provisions of this law, shall impose, as appropriate, reparation measures and guarantees of non-repetition on internet intermediaries found to have engaged in the conduct set forth in articles 53 and 60. Such measures may include, among others:

a. The publication, at the expense of the sanctioned intermediary, of an excerpt of the sanctioning decision in nationally and regionally circulated media and on its official website for a period of not less than one (1) month and not more than one (1) year;
b. The obligation to submit periodic reports detailing the measures adopted within the company and their impacts, to prevent the recurrence of conduct similar to that which gave rise to the sanction;
c. The review and modification of algorithms, technological tools, or internal policies that directly or indirectly contributed to the commission of the sanctioned conduct;
d. The temporary or permanent suspension of specific functionalities, services, or technical mechanisms that have facilitated the repeated commission of acts of gender-based digital violence against women, where adequate safeguards to ensure their safe use are not in place;
e. The obligation to cooperate in public awareness and prevention campaigns on gender-based digital violence against women, under the guidance of the competent authorities.

Article 63. Differentiated Measures for Perpetrators who are Children and Adolescents in Cases of Gender-Based Digital Violence Against Women

For the purposes of this Article, a child or adolescent perpetrator refers to any person under eighteen (18) years of age. When acts of gender-based digital violence against women are committed by such persons, the competent authorities shall apply differentiated restorative and socio-educational measures within the framework of the comprehensive child and adolescent protection system, with full respect for the best interests of the child or adolescent, their evolving capacities, the seriousness of the acts, and the rights of the victim.

Such measures shall ensure accountability, reparation for harm caused, and the prevention of recurrence, while avoiding any form of revictimization, stigmatization, or unwarranted criminalization. These measures may include, among others:

a. Mandatory participation in awareness and training programs on gender equality, prevention of digital violence, and responsible use of digital technologies;
b. Private apologies, with a restorative character and subject to the victim's acceptance, accompanied by a reflective process supervised by qualified professionals;
c. Supervised restriction on the use of digital technologies, particularly social networks or digital platforms involved in the incidents;
d. Performance of community service with a reparative focus, aimed at violence prevention or the promotion of human rights in digital environments;
e. Individual or family psychosocial monitoring aimed at addressing risk factors and strengthening skills for non-violent coexistence;
f. Participation in restorative circles, peace circles, or other dialogue spaces aimed at conflict transformation and raising awareness of the harm caused;
g. Preparation of essays, projects, or educational presentations reflecting the child's or adolescent's learning and commitment to non-repetition;
h. Guidance and shared responsibility measures directed at parents, guardians, or those responsible for the child's care and education, to promote protective and preventive environments;
i. Institutional supervision and support, in coordination with educational or community entities, for monitoring and facilitating the social reintegration of the child or adolescent.

These measures must be applied by specialized juvenile justice or child protection bodies, in coordination with child rights protection systems, and always under the supervision of competent judicial or administrative authorities.

CHAPTER V
GENERAL PROVISIONS

Article 64. Protection of the Right to Freedom of Expression

No provision of this Law shall be interpreted or applied for the purpose of, or with the effect of, unlawfully restricting the right to freedom of expression of journalists, communicators, activists, human rights defenders, or any individual engaged in the legitimate exercise of reporting, investigation, or communication, whether in digital environments or otherwise.

Any limitation on this right shall be based on a duly reasoned judicial decision issued by a competent authority and shall strictly adhere to the principles of legality, necessity, and proportionality, in accordance with international human rights law, the tripartite test of the Inter-American Human Rights System, and the digital systemic perspective. Furthermore, any restriction shall take into account the specific nature of the digital environment and its impact on the circulation of ideas and democratic participation.

Article 65. Regulatory and Budgetary Implementation

All State entities vested with responsibilities under this Law shall:

a. Design, plan, and allocate specific and adequate budgetary resources to ensure the effective fulfillment of the obligations assigned to them under this law;
b. Participate actively, jointly, and in an intersectoral manner in the development of a unified regulation that elaborates the substantive provisions and procedures established in this Law, including criteria for institutional interoperability and mechanisms for cooperation with internet intermediaries.

Article 66. Interpretation

Nothing in this Law shall be interpreted as a restriction or limitation of the American Convention on Human Rights, the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Convention of Belém do Pará), any other international conventions or other national law that provide equal or greater protections in relation to this matter.

Article 67. Complementary Protocols

Notwithstanding the enactment of this law, the Ministry of Justice, the Office of the Attorney General, and the relevant judicial and administrative authorities shall establish specialized internal protocols within their respective institutions for the handling and investigation of cases of gender-based digital violence against women. These protocols must ensure

comprehensive protection for victims, guaranteeing access to effective reporting mechanisms, the immediate implementation of appropriate protective measures, and the timely and efficient pursuit of justice and reparation.

Article 68. Repeals

All provisions contrary to this law are hereby repealed.

OAS | MESECVI

INTER-AMERICAN MODEL LAW

to Prevent, Punish, and Eradicate Gender-Based Digital Violence against Women

With the support of

Misión Observadora Permanente de Italia
Organización de los Estados Americanos

UN WOMEN

Funded by the European Union