Comments on the Draft Inter-American Model Law to Prevent, Punish and Eradicate Digital Violence Against Women

I. Introduction

Sharing the concern over the impact of technology-facilitated violence against women on the daily lives of women and girls, as well as the challenges it poses to legal frameworks, justice systems, and the design and implementation of public policies, UN Women, UNESCO, and UNFPA have joined efforts to strengthen comprehensive responses in line with their respective mandates.

In this context, the following technical comments have been prepared on the *Draft Inter-American Model Law to Prevent, Punish and Eradicate Digital Violence Against Women*, promoted by the Follow-up Mechanism to the Belém do Pará Convention (MESECVI), with the aim of ensuring its coherence with international human rights standards, its applicability across diverse legal contexts, and its contribution to the development of sustainable, multisectoral public policies centered on the needs of women and girls.

II. General Comments

Before analyzing the draft in detail, we offer three general observations on the proposed instrument as a whole:

- The need for stronger articulation not only with broader and evolving normative frameworks on violence in digital environments, but also with international instruments on human rights and violence against women and girls;
- Aspects that could be strengthened regarding legislative drafting, the definition of key concepts, and the use of terminology;
- The prevalence of a predominantly punitive approach, which narrows the State's response to sanction-based measures.

These three issues may have significant implications for the applicability, legitimacy, and effectiveness of the proposed instrument.

1. Toward a Coherent, Rights-Based Approach to Technology-Facilitated Violence

Traditionally, legal responses to crimes in digital environments have focused on the protection of information systems, data, and digital assets—commonly referred to as "cybercrime"—through provisions that penalize unauthorized access, the use of malicious software, online fraud, and phishing. This approach is well established in international instruments such as the Convention on Cybercrime.

In recent years, however, the massive and widespread use of social media and other digital platforms has given rise to new forms of technology-facilitated violence that affect a growing number of individuals. These emerging behaviors—ranging from online harassment and doxxing to hate speech, cyberbullying, and the non-consensual

distribution of intimate images—have prompted increasing efforts by States, international organizations, and civil society actors to develop new regulatory frameworks. Many of these frameworks remain under development and raise complex debates around the scope of protection, institutional responsibilities, the safeguarding of fundamental rights, and the need to balance protection from violence with the preservation of other essential freedoms in digital spaces.

The expansion of technology-facilitated violence has revealed its multidimensional impact across various social groups. While this form of violence takes many forms, numerous studies agree that certain manifestations disproportionately and severely affect women and girls. The comprehensive responses required must begin with this acknowledgment, while also recognizing the significant harm experienced by other vulnerable groups, particularly children and adolescents. At the same time, the increasing involvement of young men as perpetrators poses specific challenges for the design of prevention and redress policies, which must be tailored to the particular trajectories and experiences of these groups.

In this context, the Draft Inter-American Model Law represents an important step forward by recognizing and proposing specific regulation for forms of violence that significantly affect women and girls in all their diversity. However, its regulatory development does not fully reflect the complexity of ongoing debates surrounding digital rights, freedom of expression, anonymity, proportionality of sanctions, and the risks associated with algorithmic surveillance. Regulating violence in digital environments demands a balanced approach—one that firmly incorporates a gender perspective while safeguarding other fundamental rights.

For these reasons, it is essential to encourage Member States to read the Model Law in conjunction with broader human rights frameworks in order to ensure comprehensive and inclusive approaches that are responsive to the evolving realities of technology-facilitated violence.

2. Observations on Legislative Drafting, Concept Definitions, and Terminology

The Draft adopts an unusually prescriptive regulatory approach for a model law, by defining bodies, procedures, and enforcement mechanisms with a level of detail that may create tensions with existing legal frameworks and institutional structures in Member States. This degree of specificity limits the flexibility to adapt the law to diverse national contexts and does not fully account for the legal and administrative heterogeneity of the region.

Such a detailed regulation may hinder implementation and, in some contexts, undermine political legitimacy—particularly in settings where no equivalent frameworks exist to address other forms of violence in digital environments. For this reason, it would be more appropriate for the text to focus on broad guiding principles that serve as a reference for national legislative development, while respecting each country's institutional capacities and specificities.

Additionally, we recommend adopting the concept of "technology-facilitated violence against women and girls" (TF VAWG), as used by United Nations agencies, which better

reflects the complexity of the phenomenon. This terminology refers to an expanding field that is not limited to strictly digital environments.

The section on definitions (Article 5) could be strengthened to enhance the internal coherence of the text and its practical applicability. As currently drafted, it includes a limited selection of terms and introduces key concepts without clear definitions, which could lead to inconsistent interpretations and excessive discretionary power. In an emerging and rapidly evolving area such as TF VAWG, conceptual clarity is essential to ensure effective implementation. At the same time, it is important to allow for adaptation to local contexts and the evolution of terminology. To balance these needs, the Model Law could incorporate flexible and forward-looking mechanisms—such as general principles, interpretative notes, or annexes—that guide its application without hindering its relevance in the face of future developments.

Furthermore, terms such as "digital governance," "algorithmic bias," and "gender-motivated expression" would benefit from at least minimal definitions to guide their application.

Although the Draft includes references to factors such as sexual orientation, gender identity, or ethno-racial background, it does not develop a sustained intersectional approach to inform its practical implementation. In digital environments—where these factors may intensify or alter the experience of violence—this omission limits the law's ability to provide effective and context-sensitive responses.

In particular, the following gaps are identified:

- isolated mention of certain groups without integrating them into a coherent framework for differentiated attention;
- lack of identification of specific impacts and the barriers these groups face in accessing justice and protection;
- and the absence of measures adapted to rural contexts, as well as to Indigenous women, Afro-descendant women, youth, women with disabilities, and migrant women.

This omission represents a missed opportunity to consolidate an inclusive approach capable of addressing the diverse realities faced by women and girls in digital spaces.

3. Predominance of a Punitive Approach

Although the text formally adheres to the principle of minimal criminal law intervention (Article 4, item o), the body of the draft adopts a strongly punitive approach. It proposes criminalizing a wide range of behaviors as public offenses, without adequately distinguishing their level of severity or the type of harm caused. This orientation tends to judicialize situations that could be addressed through other mechanisms, such as administrative, educational, community-based, or restorative measures.

The lack of complementarity with preventive and transformative approaches weakens the law's potential and risks reproducing ineffective responses to promote change in the social norms that legitimize violence.

III. Specific Comments

The following are specific comments on the provisions of the Draft Law, with the aim of contributing to its improvement and facilitating its practical implementation.

1. Aspects to Improve in Legislative Drafting, Definitions, and the Formulation of Manifestations of Violence

From a legislative drafting perspective, the Draft Law contains areas that could be improved, especially regarding the definition of key concepts and the way in which the behaviors intended to be penalized as manifestations of violence are described. These issues affect the precision of the text and may lead to interpretive ambiguities or challenges in its application across different contexts.

a) Improvements to the Definitions Section (Article 5)

The definitions section contains a limited set of terms and omits several fundamental concepts that later appear in the text without a prior framework that defines their scope. For example, expressions such as "digital governance" (Art. 4, item f), "misogynistic language," "algorithmic bias," or "illegal actions" are used without a clear definition to guide their legal interpretation. This lack of precision may lead to ambiguities that hinder consistent implementation and enforcement of the law.

Given the emerging and dynamic nature of the phenomenon to be regulated, it is essential to include clear, understandable, and operational definitions. These should offer a common baseline that facilitates adaptation to different legal systems in the region, avoiding arbitrary interpretations and ensuring a minimum level of interpretive coherence.

b) Improvements to the Wording of "Manifestations of Digital Violence" (Articles 7 and 8)

Article 7, which lists "manifestations of digital violence against women on the basis of gender," includes normative descriptions that in many cases are vague or imprecise, particularly from a criminal law perspective. Several subparagraphs combine multiple verbs in a single sentence, making it difficult to clearly distinguish the different behaviors being criminalized.

Some illustrative examples include:

- **Item d):** refers to "manipulating, deceiving or exploiting a woman to send intimate sexual images, videos or messages." The term "exploiting," without a more precise definition, could encompass situations mediated by widely used commercial platforms, creating risks of overregulation or disproportionate criminalization.

- **Item e):** describes behaviors related to human trafficking, already covered under existing legislation. However, it introduces new formulations that may complicate their classification and legal proof.
- **Item g):** criminalizes the use of "spyware" without specifying the context, purpose, or actors involved. This could potentially include legitimate uses, such as household security systems.
- **Item j):** includes the possession of material involving girls (and boys), a behavior already criminalized in most national legal systems, which may lead to legal redundancy.
- **Item l):** uses terms such as "humiliate" or "degrade," which lack precise legal definitions and fail to establish clear thresholds for criminal intervention.

Article 8, for its part, adds a valuable dimension by highlighting forms of digital violence targeting women with public voices, representing significant progress in recognizing this issue. However, some of its provisions could benefit from greater precision to ensure their applicability and alignment with fundamental rights standards. For example:

- **Item b):** refers to the use of "misogynistic, sexist, racist language or incitement to violence or similar behaviors" without establishing clear criteria to distinguish between protected speech and expressions that constitute violence or unlawful incitement.
- Other provisions, such as the prohibition on "publishing false or malicious content" or "sending messages with the purpose or effect of annulling political rights," do not define thresholds of severity or evidentiary requirements.

Both articles list manifestations of technology-facilitated digital violence without classifying the behaviors according to their severity, type of harm, or the institutional response required (criminal, administrative, or restorative). This lack of differentiation hinders proper normative prioritization and may lead to disproportionate responses to very different situations. Articles 7 and 8 do not establish sufficient legal criteria to clearly define which behaviors warrant criminal sanctions and which—although socially reprehensible—do not justify the use of criminal law.

In this regard, it is recommended that the closed-list approach be replaced with a guiding enumeration, grouping behaviors into differentiated categories based on their level of harm and the expected institutional response. This strategy would help diversify State intervention mechanisms, avoid overregulation, and support better alignment with each country's legal traditions, while reducing over-reliance on punitive responses.

Furthermore, one of the strengths of a model law lies in its ability to deepen the conceptual understanding of the phenomenon it seeks to address. Therefore, it is recommended to reinforce the section on definitions and key concepts as a central pillar of the text, enabling a shared and in-depth understanding of violence against women and girls facilitated by technology.

2. Considerations on the Role Assigned to Digital Service Providers (Articles 18, 19, 22, 23, and 40)

The Draft Model Law assigns a set of functions and obligations to digital service

providers which, while aiming to strengthen responses to technology-facilitated violence, raise certain concerns from a human rights perspective—particularly due to the delegation of State responsibilities to private actors without clear safeguards or oversight mechanisms.

a) Quasi-Judicial Functions Assigned to Private Actors (Article 18)

Article 18 requires service providers to immediately report to the competent authorities any "reasonable indication of digital violence against women on the basis of gender that poses a threat to their life or safety" and to provide all available information. This provision presents two main risks:

On one hand, it assigns private actors a substantive evaluative role by requiring them to determine whether specific content constitutes a serious threat to life or integrity, without clear legal criteria or adequate supervisory mechanisms.

On the other hand, it imposes a mandatory reporting obligation that does not consider the consent of the affected woman, potentially conflicting with international standards on confidentiality and the victim-centered approach explicitly recognized in Article 4 of the same draft.

b) Algorithmic Responsibility (Article 22)

Article 22 mandates that providers design and operate their algorithms in a transparent, ethical, and accessible manner, including measures to prevent digital violence against women, eliminate bias and stereotypes, and minimize the spread of harmful content. While the goals are appropriate, the article lacks clarity regarding the scope of these obligations, the applicable technical standards, and mechanisms to ensure verifiable compliance.

c) Automated Content Moderation (Article 19)

Article 19 requires the implementation of automated mechanisms to detect content that may constitute digital violence against women, followed by review by a specialized team. This provision raises significant concerns:

It does not adequately engage with ongoing global debates around freedom of expression, algorithmic bias, and intermediary liability. Automated takedowns without clear parameters or oversight mechanisms can lead to censorship, particularly in politically sensitive contexts or against dissenting voices.

The provision lacks clear definitions of the types of content to be flagged, criteria for removal, and institutional oversight mechanisms. This contrasts with international standards set by the United Nations, which require that any content moderation measure comply with principles of legality, necessity, proportionality, transparency, and due process, under independent review (UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/38/35, 2018; Rabat Plan of Action, OHCHR, 2012; UNESCO Guidelines for the Governance of Digital Platforms, 2023).

d) Sanctioning Powers and Suspension of Services (Articles 23 and 40)

Article 23 authorizes service providers to unilaterally suspend access to their platforms for users who repeatedly share content that "may constitute criminal offenses or unlawful actions" under Article 7, following a warning and evaluation by an "internal assessment team." This provision:

Delegates sanctioning powers to private actors without establishing minimum due process guarantees, such as the right to defense or access to judicial or administrative review.

Refers to Article 7 as the basis for suspension, which is particularly problematic given that it includes a broad range of behaviors of varying nature and severity, many of which are not classified as criminal offenses under existing legal frameworks.

e) Transparency, Accountability, and Multisectoral Coordination

Based on the above observations, we recommend incorporating the principles of transparency, accountability, and multisectoral participation to ensure that digital platforms not only implement moderation and prevention measures, but do so in an open, verifiable manner and in coordination with State authorities.

In this regard, the European Union's Digital Services Act (DSA) provides a valuable reference framework. The DSA requires large digital platforms to identify and mitigate systemic risks—including technology-facilitated violence against women, hate speech, and disinformation—to cooperate with competent authorities (such as data protection agencies, law enforcement, and judicial bodies) in investigating complaints, and to uphold due process and public oversight at all times. The DSA also mandates the publication of regular transparency reports on measures taken and their results, and actively promotes the participation of civil society and users in complaint mechanisms, oversight processes, and the improvement of digital environments.

Incorporating similar obligations would help strengthen a shared-responsibility approach to preventing and responding to digital violence, while ensuring minimum standards of democratic control over the actions of private intermediaries in the digital public sphere.

3. Provisions That May Exceed What Is Advisable in a Model Law (Articles 30, 32, 46)

A Model Law should provide general guidance to support States in adapting their national legislation, while respecting their legal, institutional, and administrative frameworks. From this perspective, some provisions in the Draft may introduce a level of regulatory detail that exceeds the guiding nature of the instrument and could create tensions with existing national legislation or hinder its implementation.

Specifically, the draft establishes specific structures—such as inter-institutional committees, national administrative authorities, technical units, and evaluation teams—with defined functions, composition, and mandates, without accounting for the organizational diversity of countries across the region. For example:

- Article 9(a) foresees the creation, by decree, of a multi-stakeholder committee with detailed characteristics;
- Article 40 establishes the existence of a National Administrative Authority with sanctioning powers over digital service providers;
- Articles 30, 32, and 46 call for the creation of technical bodies and specific mechanisms with defined responsibilities.

This approach may limit States' autonomy to design their own institutional responses and could result in duplication of efforts, jurisdictional conflicts, or administrative burdens that are difficult to sustain. Rather than prescribing predetermined organizational structures, the instrument would be more effective if it proposed general functional principles—such as inter-institutional coordination, technical independence, multisectoral participation, or sanctioning capacity—that each country could adapt to its specific context.

In these cases, the Draft takes on a regulatory role that may blur its intended function as a regional guiding tool and complicate its acceptance or applicability across diverse settings.

4. **Complementary Approaches and Guidance for Non-Punitive, Comprehensive Responses**

Although the Draft Model Law acknowledges the need to adopt a human rights-based and gender-sensitive approach, it falls short of proposing a truly comprehensive framework that balances prevention, protection, and redress, or that includes alternatives to the criminal justice system.

a) Predominance of a Punitive Approach and Absence of Restorative or Community-Based Alternatives

The draft dedicates several articles to the definition of offenses and criminal procedures, giving the instrument a markedly punitive orientation. This focus is not matched by a comparable development of strategies for prevention, redress, or restorative justice. This contrasts with other regulatory frameworks on violence against women—such as the various comprehensive laws adopted in the region—which typically place greater emphasis on non-criminal components of their approach.

Although the draft mentions restorative justice, the reference is merely declarative and is not accompanied by criteria to guide its implementation. It does not establish:

- in which cases a restorative approach could be applied;
- what its objectives would be (e.g., symbolic reparation, guarantees of non-repetition, restorative dialogue processes between adolescents and youth);
- the role of educational institutions in situations involving adolescents or school communities;
- or the role of psychosocial and mental health services in addressing the psychological harm caused by technology-facilitated violence against women, independently of the legal or reporting process.

Given the complexity of the phenomena being regulated, the Draft should include clear guidance to complement criminal justice interventions with restorative or community-based mechanisms, particularly in cases where such alternatives may be more effective or more appropriate from the perspective of affected women.

b) *Weak Development of Prevention Strategies (Article 9)*

This imbalance is also evident in the limited treatment of prevention. Article 9 outlines general directives—such as the creation of inter-institutional platforms, capacity building for public officials, and awareness campaigns—but does not articulate guiding principles for the design and implementation of prevention policies.

The text does not define thematic priorities or key target populations, nor does it build on lessons learned and good practices developed in the region. It also fails to integrate prevention with essential components such as rights-based digital literacy, work within educational and community settings, or the strengthening of institutional capacities to identify and address risk situations. Six particularly relevant omissions can be identified:

- lack of emphasis on preventive work with children, adolescents, and youth;
- absence of differentiated strategies based on age, social context, and access to technology;
- weak coordination between public and private actors in prevention initiatives;
- while the Model Law rightly promotes "the implementation of measures to advance digital literacy at all levels of the educational curriculum, ensuring equitable and responsible access to technology and encouraging the active and safe participation of women, girls and adolescents in digital spaces," it would be important to clarify that educational systems should include TF VAWG not only within digital literacy content but also within broader prevention frameworks on all forms of violence against women;
- TF VAWG should be addressed as part of the broader continuum of violence against women (VAW). Therefore, VAW prevention strategies and public policies must include TF VAWG rather than establishing parallel mechanisms or duplicating efforts. It is worth assessing whether the creation of new coordination bodies is necessary, or whether it would be more effective to ensure the inclusion of TF VAWG within existing coordination structures;
- Regarding subsection d. on the training of public officials, greater clarity is needed on which sectors should be included. In particular, it is recommended that teachers, case managers working on VAW, police, prosecutors, judicial officials, and healthcare professionals receive specialized training on TF VAWG. This would help ensure that the response is not limited to the judicial sphere, but instead adopts a multisectoral approach.

Furthermore, since a significant proportion of TF VAW victims are adolescents and young women who may report through child protection systems, it is essential to include those actors among the target groups for training. These trainings should not be sporadic but part of a sustained and coordinated institutional effort aimed at improving both prevention and response to VAW across its online–offline continuum.

As a result, the preventive dimension risks being limited to symbolic or low-impact actions, without meaningful transformative capacity.

c) Provisions with Limited Guiding Value (Article 38)

Article 38, concerning "obstruction of justice," addresses a relevant issue in the context of digital violence, pointing to the challenges faced by judicial systems in cases involving technology-based offenses. However, the wording is vague and fails to provide practical guidance for justice system actors, legislators, or policymakers. To serve as an effective guiding provision, the article should identify:

- types of obstruction specific to digital environments;
- common challenges in collecting and preserving digital evidence; and
- measures to protect victims' information and rights throughout the legal process.

Including these elements would strengthen the justice system's capacity to respond and offer useful tools for designing public policies suited to the challenges of digital environments.

d) Lack of Integration with Other Public Policies

Technology-facilitated violence against women and girls cannot be addressed exclusively through a criminal justice lens. It requires active coordination with public policies in areas such as education, mental health, digital literacy, social inclusion, communication, and community development.

The draft, however, does not establish principles to promote such cross-sectoral integration, nor does it frame TF VAWG as a continuum that spans both online and offline spaces. This represents a missed opportunity to propose a comprehensive and transformative approach that connects prevention, protection, support, redress, and sanction as interdependent dimensions of a unified public policy framework.

e) Lack of Clarity on Information Management and TFGBV Data Generation (Article 9)

In subsections f. and g. of Article 9, related to data and information management, it would be important to specify that administrative VAW registries, prevalence surveys on VAW, and violence modules included in DHS and MICS surveys should incorporate questions to identify the prevalence and incidence of TF VAWG as an emerging form of violence against women and girls. Without such specifications, data systems could be duplicated rather than integrated—when the objective should be to ensure interoperable and comprehensive data systems that enable a full understanding of the scope and nature of TF VAWG.