

# **Response to call for inputs on technology-facilitated gender-based violence and its impact on women and girls for the study of the Human Rights Council Advisory Committee on technology-facilitated gender-based violence (HRC resolution 56/19)<sup>1</sup>**

February, 2025

Author: Marina Meira

Review: Paloma Lara-Castro

Derechos Digitales<sup>2</sup> is an independent non-profit latin american organization founded in 2005, whose mission is the defense, promotion, and development of fundamental rights in digital environments in Latin America. Technology facilitated gender-based violence has been one important focus of the organization's work in the past years. This contribution is therefore based on the previous and continuous research conducted by Derechos Digitales and provides insights from the Latin American context.

## **1. Which human rights are negatively impacted by technology-facilitated gender-based violence (hereafter: TFGBV) against women and girls? Identify the most impacted rights and briefly explain why.**

Technology-facilitated gender-based violence (TFGBV) is a structural human rights violation rooted in gender-based discrimination. It constitutes a direct violation of multiple human rights, as recognized by international human rights law, from which the most impacted ones include:

- **Right to live free from violence and discrimination**

As foreseen in the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and Office of the United Nations High Commissioner on Human Rights' (OHCHR) General recommendation No. 35 on gender-based violence against women

TFGBV is an extension of offline gender-based violence and stems from systemic discrimination. Women and girls, particularly those from marginalized groups are disproportionately targeted, limiting their ability to participate fully in society<sup>3</sup>. The repercussions of TFGBV go beyond the online environment, generating serious threats to the safety and physical integrity of women and LGBTQIA+ people. This type of violence may cause psychological damage, affect social relationships,

---

<sup>1</sup> OHCHR. Call for inputs. <https://www.ohchr.org/en/calls-for-input/2025/call-inputs-study-human-rights-council-advisory-committee-technology>

<sup>2</sup> More information at: <https://www.derechosdigitales.org/>

<sup>3</sup> General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35, 26 July 2017.

encourage sexual and physical violence, and in extreme cases can even lead to femicide<sup>4</sup>.

- **Right to freedom of expression and access to information**

As foreseen in the Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR)

TFGBV in many of its forms silences women's voices in the digital public sphere. Many self-censor or withdraw from online spaces due to fear of violence, limiting democratic participation and diversity in public debate<sup>5</sup>.

- **Right to privacy and data protection**

As foreseen in the ICCPR and recognized by the UN Special Rapporteur on Privacy

TFGBV frequently involves doxxing, non-consensual dissemination of intimate images (NCDII), and other forms of digital surveillance. Women's personal data, including addresses, contact details, and private communications, are weaponized to intimidate, harass, and harm them<sup>6</sup>.

- **Right to participate in political and public life**

As foreseen in the CEDAW

Women politicians, journalists, and activists are greater targets of TFGBV. They face violence in forms such as gendered disinformation, cyber mobs, and coordinated online attacks, which disproportionately affect their ability to engage in political discourse and leadership roles<sup>7</sup>.

- **Right to work and economic security**

As foreseen in the UDHR and International Labor Organization (ILO) Conventions on Workplace Harassment

Digital violence, such as workplace cyber harassment or economic abuse through identity theft and financial fraud, disproportionately affects women's employment and career advancement. Fear of online abuse deters many from public-facing roles<sup>8</sup>.

- **Right to health, including mental health**

As foreseen in the International Covenant on Economic Social and Cultural Rights (ICESCR)

TFGBV may lead to psychological distress, anxiety, depression, and suicidal ideation

---

<sup>4</sup> UNFPA. 2022 Global Symposium on Technology-facilitated Gender-based Violence Results: Building a Common Pathway.

[https://www.unfpa.org/sites/default/files/pub-pdf/TF%20GBV%20Final%20Publication\\_7.pdf](https://www.unfpa.org/sites/default/files/pub-pdf/TF%20GBV%20Final%20Publication_7.pdf)

<sup>5</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/76/258, 30 July 2021.

<sup>6</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47, 18 June 2018.

<sup>7</sup> Ibid.

<sup>8</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47, 18 June 2018.

among survivors. The long-term mental health effects are particularly severe due to the persistent and borderless nature of gender-based violence<sup>9</sup>.

- **Right to access justice and effective remedies (Article 8, UDHR; CEDAW General Recommendation No. 33)**

Survivors of TFGBV face legal and institutional barriers in seeking justice. Law enforcement often lacks the training to address TFGBV, and judicial systems trivialize or dismiss complaints. Many legal frameworks focus on criminalization rather than victim-centered approaches, failing to provide adequate remedies<sup>10</sup>. At the same time, while cybercrime regulations are multiplying around the world, they are not only ineffective in protecting the expression of women and LGBTQIA+ people, but also put them at risk – even more so in those countries where there are cultural and/or legal restrictions against certain gender expressions<sup>11</sup>.

## **2. Which specific groups within the wider population of women and girls are at risk of experiencing TFGBV (including on the basis of personal or group characteristics, professional occupation or contextual factors)?**

Certain groups of women and girls face heightened risks of TFGBV due to intersectional discrimination, professional exposure, and contextual vulnerabilities. Empirical research and case studies from Latin America provide key evidence on the groups most affected:

- Women and girls with intersecting identities face disproportionate levels of TFGBV due to the compounded effects of gender, race, ethnicity, sexuality, and socioeconomic status.
  - Indigenous and afro-descendant women are among the most affected. Indigenous women, particularly those engaged in activism, frequently experience racialized and gendered online violence. In Ecuador, Indigenous land defenders have been targets of cyber surveillance, online harassment, and disinformation campaigns used as intimidation tactics to silence their advocacy<sup>12</sup>. Similarly, afro-Brazilian women in politics face disproportionate levels of hate speech and racialized misogyny, limiting their participation in public debates and discouraging them from seeking leadership roles<sup>13</sup>.
  - LGBTQIA+ women and gender-diverse individuals are also at heightened risk of TFGBV. Online hate speech, doxxing, and cyber harassment are

---

<sup>9</sup> Accelerating efforts to eliminate violence against women: preventing and responding to violence against women and girls, with a particular focus on domestic violence, A/HRC/RES/38/5, 17 July 2018.

<sup>10</sup> Hiperderecho. (2021). Después de la Ley: Informe Nro 3. [https://hiperderecho.org/wp-content/uploads/2021/08/Informe-3\\_Despues-de-la-ley.pdf](https://hiperderecho.org/wp-content/uploads/2021/08/Informe-3_Despues-de-la-ley.pdf)

<sup>11</sup> DERECHOS DIGITALES, APC. 2023. When Protection Becomes an Excuse for Criminalization: Gender considerations on cybercrime frameworks. [https://www.derechosdigitales.org/wp-content/uploads/gender\\_considerations\\_on\\_cybercrime.pdf](https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf)

<sup>12</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>13</sup> INSTITUTO AZMINA, INTERNETLAB, NÚCLEO JORNALISMO. MonitorA. <https://monitora.org.br/>

disproportionately directed at trans and non-binary individuals, who face higher risks of coordinated digital attacks<sup>14</sup>. In Brazil, LGBTQIA+ activists and content creators are systematically targeted with threats and explicit hate speech campaigns, leading to a climate of fear and digital exclusion<sup>15</sup>. Many LGBTQIA+ individuals across Latin America endure digital violence that escalates into real-world threats, while institutional responses remain weak or nonexistent. In this sense, it's worth noting that gender-based violence legislations - including TFGBV ones - often do not encompass transgender women, who are especially vulnerable due to intersectional issues.

- Women with disabilities are particularly vulnerable to digital fraud, online abuse, and financial exploitation through deceptive digital platforms. Research indicates that visible disabilities increase online victimization, often exposing women to cyberbullying, online impersonation, and financial scams. The lack of accessible digital safety resources further compounds their risk<sup>16</sup>.
- Migrant and refugee women in Bolivia, Brazil, and Ecuador face unique digital threats, including fraudulent job offers that result in sexual exploitation and identity theft<sup>17</sup>. Their limited digital literacy and lack of legal protections in host countries further increase their vulnerability, making it difficult for them to report or seek help when facing TFGBV.
- Women in public and political life, or women in leadership, media, and activism are frequently targeted by TFGBV, with attacks designed to silence them and deter their participation in public discourse.
  - Women journalists and media workers are particularly vulnerable, facing digital harassment, doxxing, and gendered disinformation—especially when reporting on corruption, human rights, or gender issues. In Mexico, female reporters covering political violence and organized crime are persistently subjected to cyber threats, which often escalate into physical violence. Additionally, women in journalism face higher risks of deepfake attacks and smear campaigns, aimed at damaging their credibility and professional standing, further discouraging them from engaging in investigative reporting<sup>18</sup>.
  - Women human rights defenders (WHRDs) and activists are also heavily targeted online, particularly those defending indigenous land rights and reproductive justice. Cyber surveillance and digital smear campaigns are frequently used as tools of intimidation, with many WHRDs in Latin America

---

<sup>14</sup> Suzie Dunn. (2021). "Technology-facilitated Gender-Based Violence—An Overview." CIGI Supporting a Safer Internet Paper No. 1. <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/>

<sup>15</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>16</sup> Plan International (2020), cited in [https://www.cigionline.org/static/documents/SaferInternet\\_Paper\\_no\\_1\\_coverupdate.pdf](https://www.cigionline.org/static/documents/SaferInternet_Paper_no_1_coverupdate.pdf) and Jardim, L., & Penteado, C. L. (2021)

<sup>17</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>18</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/76/258, 30 July 2021.

- facing State-backed disinformation campaigns designed to discredit and delegitimize their advocacy work<sup>19</sup>.
- Women politicians and candidates, especially black and indigenous women, are subjected to targeted digital abuse, deepfake attacks, and political disinformation as a means of undermining their campaigns and discouraging them from running for office. In Brazil, studies confirm that women in politics face disproportionate levels of online harassment, which has led to a decline in female political participation and engagement in democratic processes<sup>20</sup>.
  - Women and girls in vulnerable contexts: certain life circumstances significantly increase vulnerability to TFGBV, particularly for young girls, women in abusive relationships, and informal workers who often lack institutional protections and digital security resources.
    - Girls and adolescents face heightened risks of online grooming, sextortion, and cyberstalking, largely due to the intrinsic physical, social, emotional and mental developmental stage they are going through. A survey in Ecuador found that 37% of adolescents had experienced cyberbullying, online sexual harassment, or exposure to harmful digital content, with more than 21% of adolescent girls reporting being specifically targeted for sexual purposes online. Despite the severity of these cases, State intervention remains inadequate and often disproportionate, leaving many girls vulnerable to continued abuse<sup>21</sup>.
    - Women in abusive relationships are frequently subjected to cyberstalking, location tracking, and digital coercion, which serve as extensions of intimate partner violence. In Ecuador, survivors of domestic violence have reported cases where abusers used spyware, fake accounts, and digital blackmail to exert control, making it even more difficult for women to escape cycles of abuse<sup>22</sup>.
    - Women in informal and precarious work also experience severe forms of TFGBV, particularly sex workers and women in the gig economy, who face platform-based discrimination, financial blackmail, and doxxing. In Argentina, sex workers' digital accounts are frequently removed or suspended, restricting their financial autonomy and access to safety networks, further exposing them to economic instability and exploitation<sup>23</sup>.

**3. Are there national, regional or international norms, policy or measures, specific technologies and trends, practices or research findings you would like to highlight of particular relevance for:**

---

<sup>19</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls, A/HRC/38/47, 18 June 2018.

<sup>20</sup> INSTITUTO AZMINA, INTERNETLAB, NÚCLEO JORNALISMO. MonitorA. <https://monitora.org.br/>

<sup>21</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>22</sup> Ibid.

<sup>23</sup> IOM UN MIGRATION. World Migration Report 2024. <https://brazil.iom.int/sites/g/files/tmzbdl1496/files/documents/2024-05/world-migration-report-2024.pdf>

## a) Enabling or creating an environment for TFGBV?

Several national, regional, and international norms, policies, and practices create enabling environments for technology-facilitated gender-based violence (TFGBV). These range from legal and institutional gaps to corporate practices and technological developments that, without proper safeguards, amplify harm. Below are key areas contributing to the persistence and expansion of TFGBV:

- Gaps in national legal frameworks: despite growing awareness of TFGBV, legal and policy frameworks remain fragmented and, in some cases, reinforce harmful practices
  - Lack of explicit TFGBV recognition and gendered digital protections: many national laws fail to explicitly recognize TFGBV as a form of gender-based violence (GBV), leading to inconsistent legal responses and weak protections. Additionally, some countries criminalize online violence under broader cybercrime laws, but these laws often fail to account for gendered dynamics and may even be used against survivors (e.g., criminal defamation laws used to silence women speaking out about abuse)<sup>24</sup>.
  - Over-reliance on criminalization without survivor-centered protections: many legal frameworks focus on punitive approaches without providing preventive measures, digital literacy programs, or survivor support. Research shows that the criminal justice system often fails to address TFGBV effectively, with low prosecution rates and widespread impunity. Victims often face revictimization and high reporting burdens, discouraging them from seeking justice<sup>25</sup>.
  - Misuse of morality laws and censorship against women: in some countries, laws originally intended to combat obscenity, indecency, or defamation are weaponized against women who report abuse. In some systems, NCDII is prosecuted under obscenity laws, shifting blame onto victims rather than recognizing it as a privacy violation. In parallel, women journalists and activists are frequently targeted using vague cybercrime laws, leading to self-censorship and reduced participation in public discourse<sup>26</sup>.
- Technology companies' practices and policy gaps: digital platforms and technology companies facilitate TFGBV through weak content moderation, lack of transparency, and profit-driven incentives that prioritize engagement over safety.
  - Lack of accountability for platforms' role in enabling TFGBV: social media companies have weak or inconsistent policies for addressing online harassment, particularly gendered abuse. Studies show that platforms often fail to act on user reports of TFGBV, allowing impersonation, doxxing, and

---

<sup>24</sup> DERECHOS DIGITALES, APC. 2023. When Protection Becomes an Excuse for Criminalization: Gender considerations on cybercrime frameworks. [https://www.derechosdigitales.org/wp-content/uploads/gender\\_considerations\\_on\\_cybercrime.pdf](https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf)

<sup>25</sup> Hiperderecho. (2021). Después de la Ley: Informe Nro 2. [https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2\\_Después-de-la-ley.pdf](https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2_Después-de-la-ley.pdf)

<sup>26</sup> DERECHOS DIGITALES, APC. 2023. When Protection Becomes an Excuse for Criminalization: Gender considerations on cybercrime frameworks. [https://www.derechosdigitales.org/wp-content/uploads/gender\\_considerations\\_on\\_cybercrime.pdf](https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf)

hate speech to proliferate<sup>27</sup>. Also, algorithmic amplification favors controversial and inflammatory content, further enabling misogynistic attacks and gendered disinformation campaigns<sup>28</sup>. Research shows that hate speech in general has increased in major platforms in the past years<sup>29</sup>, a movement encompassed by the authoritarian-leaning approximation of big techs. Regarding this leaning, to mention one specific example, Meta's announcement in early 2025 of alteration in its content moderation policies involves expressly permitting users to describe LGBTQ+ people as mentally ill or abnormal and to call for their exclusion from professions, public spaces, and society based on their sexual orientation and gender identity<sup>30</sup>. At the same time, these large platforms often silence health and reproductive rights related content, violating women's right to access to information<sup>31</sup>.

- Gender bias in AI and automated content moderation: AI-based moderation often fails to detect and remove gendered violence, while disproportionately censoring feminist and LGBTQIA+ activism. Content moderation algorithms prioritize Western standards, often failing to recognize regional nuances in digital abuse<sup>32</sup>.

## **b) Preventing or eliminating TFGBV?**

Preventing and eliminating TFGBV requires comprehensive legal, policy, technological, and social measures. Some key best practices and emerging approaches that have shown effectiveness in mitigating TFGBV and supporting survivors are:

- Strengthening legal and policy frameworks adapted to local contexts: legal and policy reforms should be rights-based, survivor-centered, and intersectional. They must also be developed according to the local, national or regional context in terms of GBV and technological advancement.
  - Recognizing TFGBV as a human rights violation, as done by the United Nations Human Rights Council (HRC) Resolution 56/19, and as a form of gender-based violence is essential. Mexico City's Olimpia Law, for example, provides a strong regional example of integrating TFGBV into broader GBV legislation, explicitly defining digital violence and offering all gendered protections for TFGBV victims and ensuring consistency and enforceability.

---

<sup>27</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls, A/HRC/38/47, 18 June 2018.

<sup>28</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/76/258, 30 July 2021.

<sup>29</sup> EFECOMUNICA. 2025. El discurso de odio en X aumentó un 50% desde que la compró Elon Musk, según un estudio. <https://efe.com/mundo/2025-02-13/discurso-odio-x-elon-musk/>

<sup>30</sup> HUMAN RIGHTS CAMPAIGN. 2025. Meta's New Policies: How They Endanger LGBTQ+ Communities and Our Tips for Staying Safe Online. <https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online>

<sup>31</sup> THE NEW YORK TIMES. Abortion groups say tech companies suppress posts and accounts. 2024. <https://www.nytimes.com/2024/06/11/business/abortion-groups-tech-platforms.html>

<sup>32</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/76/258, 30 July 2021

- Adopting survivor-centered and variable legal approaches is also key. Legal responses must ensure access to justice, remedies, and social support. Alternative legal mechanisms, such as constitutional actions, civil claims, and data protection laws, provide survivors with multiple legal avenues beyond criminal prosecution.
- Holding technology companies accountable: tech companies play a central role in facilitating or mitigating TFGBV, and stronger human-rights based regulations are needed to ensure accountability and transparency.
  - Strengthening proportionate, human-rights based smart regulation<sup>33</sup>, focusing on accountability and transparency and on mitigating the risks derived from platforms' business model, is essential, as well as aligned with the UN Guiding Principles on Business and Human Rights, which emphasize that tech companies have a duty to prevent, mitigate, and remediate human rights abuses in their digital spaces.
  - Gender-sensitive AI and algorithmic accountability should also be sought, as algorithmic bias contributes to TFGBV. Human oversight and gender-sensitive AI policies are needed to prevent it and improve reporting mechanisms.
  - Stress States obligations to respect human rights within the development and deployment of AI systems, expressly emphasizing the promotion of transparency, non-discrimination and diversity throughout the entire life cycle of IA systems.
  - Incorporate human rights impact assessment and due diligence as stressed by Unesco's Recommendation and the B-Tech Project on Guiding Principles on Business and Human rights.
  - Allow and reinforce the need for civil society's meaningful participation in all international, regional and national discussions regarding technology regulation.
  - Strong data protection mechanisms can also act against TFGBV. Survivors often lack control over their digital data, making them vulnerable to doxxing, cyberstalking, and deepfake attacks. Robust data protection laws with independent authorities to oversee its application and privacy-enhancing technologies should be mandated to protect vulnerable users.
- Expanding prevention through digital literacy and awareness campaigns: is important to be clear that the goal is not to shift the burden of avoiding TFGBV onto its victims. However, a proactive approach to eliminating this type of violence must include education and awareness initiatives that empower them with the tools to navigate digital spaces safely, making sure these initiatives reach remote areas.
  - The normalization of TFGBV discourages victims from reporting abuse and enables impunity. Public campaigns, such as Mexico's

---

<sup>33</sup> Statement by Irene Khan, Special Rapporteur on the promotion and protection of freedom of opinion and expression at the 47th Session of the Human Rights Council. 2021.



#NoMásViolenciaDigital<sup>34</sup>, have successfully raised awareness and encouraged survivor-centered policy changes.

- Strengthening institutional responses: States must develop robust institutional mechanisms to respond to TFGBV effectively, which involves:
  - Capacity building for law enforcement and judiciary agents on emerging issues involving TFGBV, such as digital evidence collection and gender-sensitive investigations, avoiding victim-blaming and case dismissals.
  - Expanding support services: survivors need access to holistic support, including legal aid, psychological services, and digital self-defense resources.

### c. Supporting victims of TFGBV?

Supporting victims of TFGBV requires multi-sectoral, survivor-centered, and rights-based approaches, which involve:

- Offering survivor-centered legal and institutional responses, such as ensuring comprehensive legal protections for victims and alternative legal remedies beyond criminalization.
  - Many victims do not seek criminal prosecution due to the burden of proof, privacy concerns, and lack of institutional support<sup>35</sup>. Alternative legal pathways, such as civil claims, data protection claims, copyright tools, and constitutional actions, can often provide faster and less re-traumatizing solutions.
  - Strengthening law enforcement and judicial agents' training is also key. Many legal professionals lack training on TFGBV, leading to re-victimization, case dismissals, and failure to investigate<sup>36</sup>. Having a specific administrative body to respond to cases of TFGBV might be a path into offering time-adjusted legal mechanisms to remove harmful content.
- Digital and psychological support mechanisms for victims, such as:
  - Digital security helplines and victim assistance programs. Latin America has pioneered digital security helplines, which provide technical, legal, and psychological support to victims of TFGBV. Digital security helplines, especially for marginalized groups of women, such as Navegando Libres por la Red (Ecuador), Maria d'Ajuda (Brazil), and S.O.S. Digital Center (Bolivia), provide essential guidance on online safety and self-defense strategies. They

---

<sup>34</sup> ELMOSTRADOR. #NoMásViolenciaDigital: presentan proyecto de ley que previene, repara y sanciona situaciones de acoso online como difusión de material íntimo sin consentimiento. 2020.

<https://www.elmostrador.cl/braga/2020/11/19/nomasviolenciadigital-presentan-proyecto-de-ley-que-previene-repara-y-sanciona-situaciones-de-acoso-digital-como-difusion-de-material-intimo-sin-consentimiento/>

<sup>35</sup> Hiperderecho. (2021). Después de la Ley: Informe Nro 2. [https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2\\_Despues-de-la-ley.pdf](https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2_Despues-de-la-ley.pdf)

<sup>36</sup> TEDIC (2021). Difusión de imagen no consentida en Paraguay. <https://www.tedic.org/wp-content/uploads/2021/09/Imagen-no-consentida-Tedic-web.pdf>; Supreme Court of India (2023). Handbook on combating gender stereotypes. [https://main.sci.gov.in/pdf/LU/04092023\\_070741.pdf](https://main.sci.gov.in/pdf/LU/04092023_070741.pdf)

bridge gaps in institutional responses and offer an alternative to State-based reporting mechanisms<sup>37</sup>.

- Psychological support and trauma-informed care. TFGBV survivors experience psychological distress, social stigma, and economic harm, yet mental health services for digital violence victims are scarce<sup>38</sup>. A trauma-informed approach that provides emotional support alongside legal remedies is essential.
- Improving platform response to TFGBV reports, in a contrary movement to what major platforms have been moving to recently with announcements on content moderation platforms<sup>39</sup>, as they are failing to act on TFGBV cases, leaving victims without recourse.
  - Research shows that survivors struggle with delayed responses, content takedown refusals, and inconsistent enforcement of community guidelines<sup>40</sup>. Digital platforms must therefore improve reporting mechanisms, prioritize victim privacy, and provide emergency response teams for TFGBV cases.
- Community-led and multistakeholder approach.
  - Fostering collective and community-based responses has proven to be effective, considering that community-based advocacy and feminist digital networks have been instrumental in supporting survivors and documenting TFGBV cases. Additionally, mutual aid groups, survivor networks, and feminist organizations play a key role in providing non-institutional support. Assuring a multistakeholder approach to formulating policies so that civil society and grassroots organizations can meaningfully participate and provide their insights should lead to more protective practices.
  - Expanding access to economic and social remedies, as survivors often suffer financial and social consequences, yet few laws address the economic impact of TFGBV. Financial compensation, workplace protections, and social reintegration programs are necessary for long-term recovery.

#### **4. What are the main international and national normative, regulatory and governance gaps that you have identified as regards TFGBV and human rights?**

TFGBV is worsened by critical normative, regulatory, and governance gaps at the international, national, and platform governance levels. These gaps hinder victim access to justice, and fail to balance rights appropriately, often reinforcing systemic discrimination and gender-based oppression in digital spaces.

---

<sup>37</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>38</sup> Pollicy. (2020). Fighting Violence Against Women Online: A comparative analysis on legal frameworks in Ethiopia, Kenya, Senegal, South Africa and Uganda. [https://ogbv.pollicy.org/legal\\_analysis.pdf](https://ogbv.pollicy.org/legal_analysis.pdf)

<sup>39</sup> Lara-Castro, P. Derechos Digitales. 2025. El rol de las Big Tech en el auge del autoritarismo. <https://www.derechosdigitales.org/24797/el-rol-de-las-big-tech-en-el-auge-del-autoritarismo/>

<sup>40</sup> GBV AoR. 2024. Briefing Note on Prioritizing Safety and Support in Digital Reporting of Gender-Based Violence. <https://gbvaor.net/node/1965>

Internationally, TFGBV remains insufficiently recognized and addressed. While international human rights law acknowledges gender-based violence in digital spaces, there is no global framework specifically addressing TFGBV nor establishing concrete monitoring mechanisms to face it. The UN Human Rights Council's Resolution 56/19 recognizes TFGBV as a human rights issue and mandates further research, yet it is non-binding and doesn't offer specific guidance to States and other actors. Similarly, the CEDAW applies indirectly to TFGBV but lacks enforcement mechanisms tailored to digital harms. Additionally, most countries and regions lack legal definitions of TFGBV, leading to fragmented responses.

Nationally, most GBV national laws fail to integrate TFGBV explicitly, leaving victims unprotected under existing legal mechanisms and symbolically unassisted in terms of the recognition of what they went through as GBV. Legal frameworks are often fragmented across GBV, cybercrime, and data protection laws, creating confusion for victims seeking justice. Furthermore, current legal responses remain overly reliant on criminalization, placing high evidentiary burdens on victims, prolonging legal processes, and increasing risks of re-victimization. Women from marginalized communities face greater barriers to justice, as legal systems often trivialize digital violence, forcing victims to navigate underfunded, biased, and inefficient judicial processes.

Beyond legal gaps, governance failures in the tech industry further exacerbate TFGBV. Social media platforms consistently fail to enforce policies against TFGBV, allowing perpetrators to act with impunity. Moreover, most legal frameworks fail to impose liability on tech companies for failing to prevent and mitigate TFGBV.

## **5. What is the impact of TFGBV on the achievement of the Sustainable Development Goals (SDGs)? Identify the most impacted goals and briefly explain why.**

TFGBV has severe consequences for the achievement of the SDGs. Particularly:

- SDG 5: Gender Equality, target 5.2 – eliminate all forms of violence against women and girls: TFGBV is a direct violation of gender equality, reinforcing patriarchal oppression and gender-based violence in digital spaces.
- SDG 4: Quality Education, target 4.5 – eliminate gender disparities in education: young girls and women are disproportionately targeted for online harassment, cyberbullying, and sextortion, leading to psychological distress, social withdrawal, and school dropout. In Latin America, digital gender-based violence affects teenage girls' ability to engage in online learning spaces, limiting their access to education and information. Girls in marginalized communities face a double burden—a lack of access to digital education and higher exposure to online threats<sup>41</sup>.
- SDG 8: Decent Work and Economic Growth, target 8.5 – achieve equal pay and decent work for all women and men: women face digital discrimination, workplace

---

<sup>41</sup> Luchadoras and SocialTic. *Take Back the Tech!* (2018). <https://www.takebackthetech.net/>

cyber-harassment, and economic sabotage through identity theft, deepfake abuse, and online extortion, which affect their financial stability. Many women in informal or digital-based work (such as online freelancers, influencers, and sex workers) experience financial exclusion, as digital platforms fail to protect them from doxxing, payment blacklisting, and deplatforming. Additionally, TFGBV and reputational attacks prevent women from pursuing leadership roles or high-profile careers, limiting professional advancement<sup>42</sup>.

- SDG 10: Reduced Inequalities, target 10.2 – empower and promote the social, economic, and political inclusion of all: TFGBV disproportionately impacts marginalized women, including Indigenous, LGBTQIA+, migrant, and disabled women, further exacerbating digital divides and social exclusion. In many Latin American countries, racialized and gendered digital violence targets women journalists, politicians, and activists, reducing their access to digital spaces and silencing critical voices<sup>43</sup>.
- SDG 16: Peace, Justice, and Strong Institutions, target 16.10 – ensure public access to information and protect fundamental freedoms: TFGBV restricts women's access to free expression, public debate, and civic participation. Women journalists and human rights defenders are frequently subject to TFGBV, undermining their ability to report on corruption, human rights violations, and social issues<sup>44</sup>.

## **6. What actions at the international level would you advocate for to address these gaps and potential human rights impact?**

Any international-level action addressing TFGBV must be based on the fundamental understanding that there is no single, universal solution applicable to all contexts. While global agreements and actions aim to establish common principles and advance collective progress, they must also recognize the vast differences in regional and national realities, which require tailored responses rather than one-size-fits-all approaches. The structural inequalities between the Global North and the Global South, including economic power imbalances and disparities in symbolic representation within multilateral spaces, further highlight the need for nuanced, context-specific strategies. According to Oxfam, in 2023, the wealthiest 1% in the Global North extracted \$30 million per hour from the Global South, underscoring the power asymmetries that shape global policy discussions<sup>45</sup>.

These inequalities also manifest within individual countries, where socioeconomic, legal, and technological disparities create differentiated vulnerabilities to TFGBV. Effective responses must consider these internal and external complexities, ensuring that any global framework incorporates regional realities, local priorities, and differentiated protections for

---

<sup>42</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective (2018)

<sup>43</sup> Economist Intelligence Unit (EIU), Measuring the prevalence of online violence against women, 2020. <https://onlineviolencewomen.eiu.com/>

<sup>44</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, A/76/258, 30 July 2021

<sup>45</sup> OXFAM BRASIL. 2025. Às custas de quem? <https://www.oxfam.org.br/wp-content/uploads/2025/01/Davos-2025-Methodology-Note.pdf>

marginalized communities. Without such an approach, international efforts risk being detached from the lived experiences of those most affected by TFGBV and failing to deliver meaningful, equitable digital protections.

That said, to effectively address the gaps and mitigate the human rights impact of TFGBV, coordinated action at the international level is essential. Some key actions that could be undertaken internationally and in international spaces to address TFGBV are:

- Establishing an international framework on TFGBV, which should include legal and non legal measures, in the form of a legally binding UN convention or protocol on TFGBV or an optional protocol under CEDAW, for example. Such a framework should define TFGBV as a human rights violation, mandate legal protections and remedies for survivors and require governments to enforce platform accountability to prevent and mitigate TFGBV.
- Mainstreaming TFGBV into existing human rights mechanisms, integrating TFGBV into CEDAW reporting processes and on periodic reviews of States, ensuring that State Parties report on the issue prevention and response efforts. The UN Human Rights Council's Special Procedures and Universal Periodic Review (UPR) mechanisms should in this sense include TFGBV in their country assessments, ensuring that governments are held accountable for addressing digital gender-based violence.
- Strengthening other international and regional bodies, such as the UN Special Rapporteur on Violence Against Women and Girls or the Inter American Commission of Human Rights, to monitor and issue recommendations on TFGBV globally and regionally.
- Ensuring coherence between international frameworks, such as the recently approved UN Cybercrime Convention, by reviewing and integrating into them gender-sensitive protections.
- Strengthening tech accountability at the international level, as big techs operate globally and often have more power than some States, especially those from the Global South. Not only, but these companies tend to establish different policies for different countries or regions, offering more protection to users in regions with stronger regulation such as the European Union. It is therefore important to enforce global corporate responsibility standards, such as mandatory human rights due diligence, alongside recognizing through a binding international instrument on business and human rights that tech platforms should be held accountable for enabling gender-based violence. Establishing an international sanctions mechanism to hold accountable platforms that fail to meet minimum human rights due diligence requirements, including potential trade and financial restrictions, is also important.
- Pushing for the recognition of TFGBV as grounds for asylum, ensuring that women fleeing digital harassment, doxxing, or state-sponsored online violence can seek international protection.

- Expanding global funding for feminist organizations working to support survivors of TFGBV, such as those holding digital security helplines which provide legal, psychological, and technical assistance to victims.
- Supporting feminist digital infrastructure and alternative online spaces, investing in feminist-led digital platforms and encrypted communication tools that prioritize safety, privacy, and non-surveillance technologies. The same goes for expanding international support for feminist tech initiatives, ensuring that marginalized communities have access to safe and inclusive digital spaces.

## **7. What international organizations, bodies, or agencies are best placed to tackle TFGBV? Further, are there instances of duplication of efforts to tackle TFGBV and how do you consider this could be overcome?**

Among the United Nations, some agencies that are well positioned to work on TFGBV are: the UN Human Rights Council and Special Rapporteurs (on Violence Against Women and Girls and Freedom of Expression, notably), the UNFPA - which provides a broadly protective definition on TFGBV<sup>46</sup> -, the UN Women - considering its previous work on TFGBV in the Beijing+25 process and in collaboration with CSW67 -, and the ITU. At the regional level, for Latin America, the Inter-American Commission on Human Rights and the Follow-up Mechanism to the Belém do Pará Convention (MESECVI) should be considered. The Special Rapporteur on Freedom of Expression has previously documented topics related to TFGBV, such as attacks against women journalists and activists<sup>47</sup>.

Additionally, civil society organizations with international and/or regional work, as well as coalitions composed of them, are also well positioned to discuss future actions on tackling TFGBV. Civil society organizations are well positioned to discuss this matter because they work closely with affected communities, providing firsthand insights and support. They also advocate for policy changes, raise awareness, and push for stronger legal protections. Derechos Digitales<sup>48</sup> is one of them, situated within Latin America. AISur<sup>49</sup>, a consortium of civil society organizations from Latin America, is another one. Globally, the coalition which presented the Feminist Principles for Including Gender in the Global Digital Compact<sup>50</sup> is also notable.

Establishing a global task force on TFGBV could be a fruitful pathway into preventing the duplication of efforts on the issue and moving towards a coordination of actions to achieve broader impact. The taskforce could be composed by UN bodies such as the ones

---

<sup>46</sup> “an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media, against a person on the basis of their gender”. UNFPA. Brochure: What is Technology-Facilitated Gender-Based Violence? 2023. <https://www.unfpa.org/resources/brochure-what-technology-facilitated-gender-based-violence>

<sup>47</sup> Inter-American Commission on Human Rights (IACHR). *Special Rapporteur for Freedom of Expression Annual Report*, 2020.

<sup>48</sup> <https://www.derechosdigitales.org/>

<sup>49</sup> <https://www.alsur.lat/>

<sup>50</sup> APC. The Feminist Principles for including gender in the Global Digital Compact. 2023. <https://www.apc.org/en/pubs/feminist-principles-including-gender-global-digital-compact-0>

mentioned above, as well as regional human rights bodies and civil society organizations. Such a taskforce should promote mechanisms for the meaningful engagement of feminist and digital rights organizations, as integrating feminist digital rights expertise can lead to policies that overlook intersectional vulnerabilities. Allocating UN and regional human rights funding to grassroots initiatives, integrating these initiatives and their results to the international action-formulating process, is also important for ensuring that local expertise informs global policy.

#### **8. Are there national or regional statistics or other data on the prevalence of TFGBV available in your country provided by the public sector, national human rights institutions (NHRIs), NGOs or academia?**

There is an important lack of production and availability of national and regional statistics on the prevalence of TFGBV, which makes the formulation of policies to tackle it more difficult and less adequate. Even though TFGBV has been an object of study among Latin American human rights institutions, NGOs and academia, data collection remains fragmented and inconsistent across countries.

Some relevant national-scale data from Latin American countries:

- In Mexico, the National Survey on Victimization and Perception of Public Safety reported that women under 30 are the most vulnerable to cyberstalking and harassment<sup>51</sup>. However, the lack of specific TFGBV indicators limits the ability to assess the full scale of the issue.
- In Peru, the National Institute of Statistics and Informatics (INEI) found that 35% of women who experience online abuse also face offline gender-based violence, demonstrating a continuum between digital and physical violence<sup>52</sup>.
- In Brazil, the Brazilian Public Security Forum reported that 18.6 million women suffered violence, including cyber harassment, doxxing, and digital financial control, though the data is not fully disaggregated by type of digital abuse<sup>53</sup>.

Alongside such State-produced data, feminist and digital rights organizations provide some of the most detailed documentation of TFGBV, particularly on underreported cases and the experiences of marginalized communities. Some examples are:

---

<sup>51</sup> Información de Gobierno, Seguridad Pública e Impartición de Justicia. Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2022. <https://www.inegi.org.mx/programas/envipe/2022/>

<sup>52</sup> Instituto Nacional de Estadística e Informática (INEI), Encuesta Nacional sobre Relaciones Sociales (ENARES), 2019. [https://www.inei.gob.pe/media/MenuRecursivo/boletines/presentacion\\_enares\\_2019.pdf](https://www.inei.gob.pe/media/MenuRecursivo/boletines/presentacion_enares_2019.pdf)

<sup>53</sup> Fórum Brasileiro de Segurança Pública, Visível e Invisível: A Vitimização de Mulheres no Brasil, 2023. <https://forumseguranca.org.br/wp-content/uploads/2023/03/visiveleinvisivel-2023-relatorio.pdf>

- Derechos Digitales has conducted regional research on several themes and topics related to TFGBV<sup>54</sup> and towards a feminist approach to digital rights<sup>55</sup>.
- Luchadoras (Mexico) has documented online violence against women in politics, analyzing how gendered attacks discourage female participation in public life<sup>56</sup>.
- MariaLab (Brazil) focuses on TFGBV against LGBTQIA+ individuals and sex workers, highlighting platform discrimination and digital financial exclusion<sup>57</sup>.
- Hiperderecho (Peru) has researched the implementation of TFGBV legislation, producing relevant information on the barriers faced by victims of this type of violence, particularly regarding access to justice<sup>58</sup>.

Despite growing awareness of TFGBV in Latin America, significant gaps in data collection and accountability persist. Few countries systematically disaggregate TFGBV data in crime and GBV statistics, making it difficult to assess the full scope of the issue. Additionally, tech companies fail to provide transparent data on TFGBV reports, limiting the ability of policymakers and civil society to hold platforms accountable. Furthermore, intersectional identities—including Indigenous, Afro-descendant, LGBTQIA+, and disabled women—remain underrepresented in research, leaving the specific vulnerabilities of these groups largely unaddressed.

To strengthen TFGBV data collection in the region, it is crucial to develop standardized TFGBV indicators within national surveys, ensuring consistent and comparable statistics across countries. Tech companies must also be mandated to release gender-disaggregated transparency reports, providing clearer insights into the prevalence of digital violence and the effectiveness of content moderation. Moreover, funding for intersectional research on TFGBV targeting marginalized communities must be prioritized, ensuring that prevention and response strategies are inclusive and evidence-based.

### **8.1. If yes, what is the prevalence and types of TFGBV in your national or regional context?**

There is not enough data available to allow a broad and accurate understanding of the prevalence of types of TFGBV in Latin America. This absence of data hinders the formulation of effective public policies, as it prevents a full understanding of the scope and nature of the problem. Without accurate information, policymakers lack the necessary evidence to develop adequate prevention, protection, and response strategies, resulting in

<sup>54</sup> DERECHOS DIGITALES, APC. 2023. When Protection Becomes an Excuse for Criminalization: Gender considerations on cybercrime frameworks. [https://www.derechosdigitales.org/wp-content/uploads/gender\\_considerations\\_on\\_cybercrime.pdf](https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf);

DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>

<sup>55</sup> DERECHOS DIGITALES. Latin America in a Glimpse 2024: Reflections for a Community-Based, Feminist AI. [https://www.derechosdigitales.org/wp-content/uploads/Glimpse\\_2024\\_ENG.pdf](https://www.derechosdigitales.org/wp-content/uploads/Glimpse_2024_ENG.pdf)

<sup>56</sup> LUCHADORAS. 2018. VIOLENCIA POLÍTICA A TRAVÉS DE LAS TECNOLOGÍAS CONTRA LAS MUJERES EN MÉXICO. [https://luchadoras.mx/wp-content/uploads/2024/10/violencia\\_politica\\_a\\_traves\\_de\\_las\\_tecnologias\\_contra\\_las\\_mujeres\\_en\\_mexico\\_pags\\_web.pdf](https://luchadoras.mx/wp-content/uploads/2024/10/violencia_politica_a_traves_de_las_tecnologias_contra_las_mujeres_en_mexico_pags_web.pdf)

<sup>57</sup> <https://www.marialab.org/>

<sup>58</sup> <https://hiperderecho.org/despuesdelaley/proyecto>



fragmented and ineffective approaches. Additionally, the lack of data makes it difficult to monitor and evaluate existing initiatives, limiting the ability to adjust and improve policies as needed<sup>59</sup>.

## **8.2. What gaps in research on TFGBV exist in your country or region?**

There are persistent gaps in research on TFGBV in Latin America, directly affected by the lack of systematic data collection or gender-disaggregated data availability on the agenda in national surveys or tech companies' reports.

Research remains limited and fragmented particularly in relation to intersectional identities and the broader consequences of digital violence. There is little to no data on how Indigenous, Afro-descendant, LGBTQIA+, and disabled women experience TFGBV, despite clear evidence that these groups face heightened risks of online harassment, cyberstalking, and digital exclusion.

Beyond legal and policy gaps, the economic and psychological consequences of TFGBV remain largely unexamined. No large-scale studies in the region have assessed the financial and mental health impacts of digital violence, leaving a critical gap in understanding how survivors experience and navigate these harms. Most existing research focuses on legal frameworks and law enforcement responses, failing to capture the broader socio-economic effects and emotional toll that TFGBV has on victims' lives. Addressing these gaps is essential to developing comprehensive, survivor-centered policies that not only hold perpetrators accountable but also provide tangible support for those affected by digital violence.

## **9. Has your country introduced any policy, legislation or other initiative to address TFGBV and its impact on women and girls at the national level? If so, please share any relevant information.**

As Derechos Digitales works regionally in Latin America, to respond to this question, three countries from our region were selected as examples and will be hereafter considered: Mexico, Peru, and Brazil, which have been the subject of study in Derechos Digitales and its partners' research. Each of these three countries have introduced legislative and policy measures to address TFGBV, yet their responses remain fragmented and primarily punitive, with limited preventive efforts and weak platform accountability.

- Mexico
  - Ley Olimpia from Mexico City (Olimpia Law, from 2020): Mexico's Olimpia Law is one of the most comprehensive national measures against TFGBV, criminalizing NCDII and defining digital violence as a form of gender-based violence. The law expands protections under the Criminal Code and the Law

---

<sup>59</sup> Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém do Pará. OEA/MESECVI. 2021. [https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20lin%20ea%202.1%20%282%29\\_Aprobado%20%28Abril%202022%29\\_0.pdf](https://lac.unwomen.org/sites/default/files/2022-11/MUESTRA%20Informe%20Violencia%20en%20lin%20ea%202.1%20%282%29_Aprobado%20%28Abril%202022%29_0.pdf)

on Women's Access to a Life Free of Violence (LAVLV), addressing cyber harassment, doxxing, and online sexual extortion. It also provides victims with the right to demand the removal of harmful content and access legal, psychological, and social support services. However, it lacks provisions for digital privacy, data protection, and platform liability, and its remedies focus on punitive justice rather than holistic victim support.

- Additional Government and Civil Society Initiatives: the Mexican National Human Rights Commission has advocated for stronger protections against digital violence, calling for greater regulation of social media platforms<sup>60</sup>. Meanwhile, organizations such as the Red Nacional de Refugios provide survivors with digital security training and legal aid, bridging gaps in institutional responses<sup>61</sup>.
- Peru
  - Legislative Decree 1410 (2018): this law criminalizes online harassment, cyberstalking, sexual blackmail, and NCDII, acknowledging TFGBV as a growing issue. However, it remains disconnected from Peru's broader gender-based violence frameworks, limiting the ability to provide coordinated protections. Moreover, it focuses on criminal prosecution without mechanisms for content takedown, reparation, or digital safety assistance.
  - National Plan Against Gender-Based Violence: The 2016-2021<sup>62</sup> plan recognized the role of technology in GBV but failed to implement concrete digital safety measures.
  - Civil society initiatives: Digital rights organizations in Peru such as Hiperderecho continue to push for stronger TFGBV protections.
- Brazil
  - Legal Responses to TFGBV: unlike Mexico and Peru, Brazil lacks a unified national law addressing TFGBV. Instead, digital gender-based violence is addressed through general cybercrime and gender-based violence laws, including: Law 12.737 (Carolina Dieckmann Law, 2012), which Criminalizes unauthorized access to private data, though it does not explicitly cover TFGBV; Law 13.718 (2018), which recognizes sexual harassment and NCDII but lacks digital-specific protections; and the Maria da Penha Law (2006), Brazil's primary GBV law, which does not explicitly address digital violence.
  - Government and NGO Efforts: The Maria d'Ajuda helpline<sup>63</sup> provides direct support for TFGBV survivors, including assistance with account takeovers, doxxing, and digital harassment.

**in particular, has your country implemented any action on:**

<sup>60</sup> Comisión Nacional de los Derechos Humanos (CNDH), México. Recomendaciones sobre violencia digital y regulación de plataformas, 2022. <https://www.cndh.org.mx/documento/recomendacion-1542022>

<sup>61</sup> <https://rednacionalderefugios.org.mx/>

<sup>62</sup> LIBRARY OF CONGRESS. Peru: National Plan on Gender-Based Violence 2016-2021 Approved. <https://www.loc.gov/item/global-legal-monitor/2016-09-01/peru-national-plan-on-gender-based-violence-2016-2021-approved/>

<sup>63</sup> <https://mariadajuda.org/>

**a. Technology-facilitated gender-based sexual violence?**

- Mexico: Ley Olimpia criminalizes NCDII and online sexual harassment, granting victims the right to request content removal and seek legal aid. However, it relies primarily on punitive measures rather than survivor-centered approaches.
- Peru: Legislative Decree 1410 criminalizes online sexual harassment and blackmail, while the National Plan Against GBV (2022-2027) acknowledges digital sexual violence but lacks specific survivor protections or platform regulations.
- Brazil: Law 13.718 (2018) penalizes online sexual harassment but does not explicitly include TFGBV protections. The Maria d'Ajuda helpline assists victims of revenge porn and digital sexual abuse, but systemic legal gaps remain.

**b. Technology-facilitated gender-based harassment and bullying?**

- Mexico: Ley Olimpia covers online harassment, but its enforcement remains weak, and many forms of digital abuse remain outside its scope.
- Peru: Legislative Decree 1410 addresses cyber harassment, yet enforcement remains inconsistent, with many cases underreported or dismissed.
- Brazil: There is no specific law against online harassment. Law 14.811 from 2024 criminalized bullying and cyberbullying, however it doesn't present any gender distinction or stream.

**c. Technology-facilitated gender-based trafficking and exploitation?**

- Mexico: The General Law on Human Trafficking (2012, updated 2019) recognizes digital exploitation, yet it does not account for emerging TFGBV forms such as AI-generated deepfake abuse. Social media platforms and encrypted apps are frequently used for trafficking, yet platform accountability remains weak.
- Peru: The National Plan Against Human Trafficking (2017-2021) includes online-facilitated trafficking, yet enforcement remains limited, and there are no binding platform regulations to prevent trafficking-related TFGBV.
- Brazil: Law 13.344 (2016) criminalizes human trafficking, including digital-facilitated exploitation, but lacks strong enforcement mechanisms.

**d. Technology-facilitated gender-based privacy violations?**

- Mexico: Ley Olimpia from Mexico City criminalizes doxxing and unauthorized access to private images, yet it does not mandate tech companies to proactively prevent privacy violations.
- Peru: Legislative Decree 1410 criminalizes NCDII.
- Brazil: The General Data Protection Law (LGPD, 2018) provides privacy protections, but it does not contain TFGBV-specific measures. Law 13.718 from 2018, in its turn, criminalizes the disclosure of rape scenes or scenes of rape of a vulnerable person, sex scenes or pornography.

## **10. Are there national or regional initiatives that address specific groups of women and girls?**

Considering Mexico, Peru and Brazil, there is an important lack of initiatives to address TFGBV against specific groups of women and girls, especially State-led ones. Even though the existing ones are insufficient, some actions are worth mentioning:

- Mexico
  - Ley Olimpia recognizes digital violence as a form of gender-based violence and has been instrumental in protecting women against online sexual harassment and NCDII.
  - The Mexican National Human Rights Commission has issued recommendations to improve protections for Indigenous and LGBTQIA+ communities, who face heightened digital violence risks<sup>64</sup>.
- Peru
  - Legislative Decree 1410 criminalizes online harassment and sexual exploitation, but does not explicitly address marginalized groups.
  - The National Plan Against Gender-Based Violence (2022-2027) aims to improve legal protections for women in vulnerable communities.
- Brazil
  - The Maria da Penha Law (2006) covers gender-based violence but does not explicitly include digital forms of abuse nor any kind of specific group of women.
  - Feminist civil society initiatives like Maria d'Ajuda provide digital security services for marginalized women.

## **11. From a human rights perspective, what are the key regulatory and legislative gaps at the national level? In addition, what new legal or other measures are required to address TFGBV and what obstacles hinder their implementation?**

The legal and regulatory national frameworks in Latin America - and more specifically in Mexico, Peru and Brazil - remain insufficient to effectively address TFGBV, with significant gaps that leave many survivors without adequate protection or access to justice. One of the key shortcomings is the lack of intersectional protections. Most TFGBV laws fail to explicitly recognize the heightened risks faced by Indigenous, LGBTQIA+, and disabled women, leaving these communities without tailored legal safeguards. Additionally, existing frameworks, with the exception of Mexico City's Olympia Law, are not fully integrated into broader gender-based violence laws, which means that digital violence is often treated as a separate issue rather than part of the continuum of gender-based violence that disproportionately affects marginalized groups.

---

<sup>64</sup> Comisión Nacional de los Derechos Humanos (CNDH), México. Recomendaciones sobre violencia digital y protección de comunidades indígenas y LGBTQIA+, 2022. <https://www.cndh.org.mx/palabras-clave/1505/lgbttti>

Another major challenge is the absence of binding regulations that hold technology platforms accountable. No laws in the region currently mandate social media companies to take responsibility for TFGBV cases, nor do they require platforms to disclose the number of reports they receive or their enforcement actions. As a result, survivors face significant barriers when trying to report and remove harmful content, while perpetrators act with near impunity. Furthermore, most legal responses to TFGBV rely heavily on criminalization, focusing on punishing offenders rather than providing survivor-centered support, prevention mechanisms, or non-criminal legal remedies. Few countries offer alternative forms of justice, such as civil, administrative, or regulatory avenues, leaving victims with limited options beyond the often slow and retraumatizing criminal justice system.

To close these gaps, it is essential to expand legal responses beyond criminalization, from an approach that favours proportionality and a balance of rights, ensuring that survivors have access to civil and administrative remedies, including emergency content takedown mechanisms, digital security support, and legal aid services. Governments must also mandate greater transparency from tech companies, requiring them to publicly report TFGBV cases, improve content moderation systems, and implement stronger protections for victims. Additionally, intersectional legal frameworks must be developed to explicitly address the vulnerabilities of Indigenous, LGBTQIA+, and disabled women, ensuring that TFGBV protections are truly inclusive and responsive to the diverse realities of digital violence in Latin America.

## **12. What specific mechanisms are in place to support victims of TFGBV? In particular:**

### **a) What current legal remedies and actions are available for victims of TFGBV in your country?**

- Mexico: Ley Olimpia from Mexico City provides legal mechanisms for content removal and psychological support, as it is integrated with the previous GBV legal framework.
- Peru: Legislative Decree 1410 criminalizes TFGBV but requires victims to file private complaints, making justice often inaccessible. It doesn't foresee any kind of remedy to victims.
- Brazil: No. The legal framework for TFGBV in Brazil is essentially criminal and doesn't foresee any remedies to victims. Given that the main GBV legal framework (Maria da Penha Law) doesn't encompass TFGBV, victims are not entitled access to remedies foreseen in such legislation.

### **b) Are there specific authorities or entities, such as equality bodies or NGOs, that support victims of TFGBV at the national level? If so, how do they tackle TFGBV and support victims?**

Considering Mexico, Peru and Brazil, none of these countries has one institutional body fully and specifically dedicated to supporting TFGBV victims. They find, however, dispersed support among governmental and non-governmental spaces:

- Mexico:

- The Secretariat of Women of Mexico City offers psychological, medical, social service and legal support to victims of GBV<sup>65</sup>.
- According to Mexico City's Olimpia Law, NCDII is prosecuted by the Public Ministry, which should support legal assistance to the victim.
- The civil society organization Red Nacional de Refugios provides digital security training for TFGBV survivors, as well as psychological and health support<sup>66</sup>.
- Peru:
  - The Ministry of Women and Vulnerable Populations offers psychosocial support to victims, but lacks digital security programs.
  - The Legislative Decree 1410 adds the offense of unconsented dissemination of sexual content to a chapter of the Criminal Code in which the crimes are prosecuted by private criminal proceedings. That means that the victim must assume the responsibility of investigating, collecting evidence and presenting her theory of the case before the Judiciary, instead of the Public Ministry.
  - The offenses of harassment, sexual harassment and sexual blackmail, on the other hand, are prosecuted by the Public Ministry, once the victim presses charges.
- Brazil:
  - It is not clear whether TFGBV claims - given their criminal nature in Brazil - should be filed in cybercrime or gender crime police divisions.
  - Despite this problem, all victims of GBV (which doesn't explicitly encompass TFGBV, but it could be understood so) in Brazil can access free legal support through the Public Defender's Office.
  - SaferNet Brasil is a civil society association which offers a service for receiving anonymous reports of crimes and violations against human rights on the internet. Their hotline<sup>67</sup> was structured through a partnership with police and judicial authorities and they are the national organization working in Brazil working in partnership with the National Center for Missing and Exploited Children (NCMEC)<sup>68</sup>. Among the complaints one can report are violence or discrimination against women, child pornography<sup>69</sup> and LGBTfobia.

**13. Is your country collaborating at the international level with regional or international organizations to address TFGBV? If yes, specify which organizations and provide relevant information if possible.**

---

<sup>65</sup>

[https://data.consejeria.cdmx.gob.mx/images/leyes/leyes/LEY\\_DE\\_ACCESO\\_DE\\_LAS\\_MUJERES\\_A\\_UNA\\_VIDA\\_LIBRE\\_DE\\_VIOLENCIA\\_DE\\_LA\\_CDMX\\_8.7.pdf](https://data.consejeria.cdmx.gob.mx/images/leyes/leyes/LEY_DE_ACCESO_DE_LAS_MUJERES_A_UNA_VIDA_LIBRE_DE_VIOLENCIA_DE_LA_CDMX_8.7.pdf)

<sup>66</sup> <https://rednacionalderefugios.org.mx/>

<sup>67</sup> <https://new.safernet.org.br/denuncie#>

<sup>68</sup> NCMEC proactively provides assistance to victims, families, law enforcement, social service agencies, mental health agencies and others when they need help with a missing, exploited or recovered child. Processing complaints against child sexual abuse material is among the organization's work.

<sup>69</sup> The most adequate term is child sexual exploitation, but the hotline uses "child pornography".

Mexico, Peru, and Brazil have each engaged in international collaborations to address TFGBV, though their levels of commitment and impact vary. They have participated in global gender discussions in multilateral spaces, including the Commission on the Status of Women (CSW), where they have supported calls for digital safety measures and stronger protections for women in online spaces. Debates surrounding the Global Digital Compact (GDC) have raised concerns about the need for gender-sensitive approaches to digital governance, with feminist organizations from throughout the world pushing for stronger regional representation and more inclusive policy discussions. While these countries contribute to international TFGBV debates, this theme hasn't been a priority for any of them. Gaps remain in translating these commitments into binding national regulations, and ensuring that TFGBV remains a central issue in global digital governance discussions, as well as in particular regions such as Latin America.

#### **14. Are there any specific technology, industry practices or policies relevant that either enable, increase, prevent or tackle TFGBV?**

Technology plays a dual role in GBV—it can exacerbate it while also providing tools for prevention, protection and care<sup>70</sup>. The business model of big tech platforms, which prioritizes data extraction, engagement-driven algorithms, and self-regulated moderation, is one of the primary enablers of TFGBV. Social media platforms, search engines, and messaging apps operate on an advertising-based economy that profits from user engagement, regardless of whether that engagement is driven by positive interactions or harmful content. This structural incentive problem leads to deliberate design choices that amplify misogynistic abuse, disinformation, and gendered harassment while deprioritizing user safety and privacy.

This data-based and problematic business model is not exactly new, however big tech companies have been becoming more authoritarian and less protective of human rights in the past years. One of the clearest examples of this trend is Elon Musk's transformation of X (formerly Twitter). Since acquiring the platform, Musk has dismantled trust and safety teams, reinstated accounts known for harassment and disinformation, and introduced a paid verification system (X Premium) that artificially boosts visibility for those willing to pay, including perpetrators of TFGBV<sup>71</sup>. By weakening content moderation and monetizing virality over accuracy or ethical responsibility, X has become a more hostile space for women, LGBTQIA+ individuals, and marginalized communities<sup>72</sup>.

Similarly, Meta recently announced a policy change which can lead to political figures to spread misinformation on its platforms, including on topics like gender rights, reproductive justice, and LGBTQIA+ issues, further contributing to the spread of gendered disinformation

---

<sup>70</sup> UN – Human Rights Council. (2013). Report of the Working Group on the issue of discrimination against women in law and in practice. A/HRC/23/50. Paras. 48 and 66.

<sup>71</sup> NPR. Musk's Twitter has dissolved its Trust and Safety Council. 2022. [https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk?utm\\_source=chatgpt.com](https://www.npr.org/2022/12/12/1142399312/twitter-trust-and-safety-council-elon-musk?utm_source=chatgpt.com)

<sup>72</sup> EFECOMUNICA. 2025. El discurso de odio en X aumentó un 50% desde que la compró Elon Musk, según un estudio. <https://efe.com/mundo/2025-02-13/discurso-odio-x-elon-musk/>

and targeted abuse campaigns<sup>73</sup>. These changes do not happen in isolation—they reflect the fundamental conflict of interest between big tech’s profit motives and user safety.

Additionally, data exploitation and breaches play a key role in facilitating TFGBV. Platforms routinely harvest massive amounts of personal data—including location, behavioral patterns, and private communications—to optimize targeted advertising. However, this data is often mishandled, leaked, or exploited, exposing users, especially women and gender-diverse individuals, to cyberstalking, doxing, and intimate image abuse. Cases such as the Cambridge Analytica scandal and recurring Meta data breaches demonstrate that big tech’s self-regulated security practices are inadequate, creating systemic vulnerabilities that enable TFGBV on a large scale.

In short, the dominant business model of big tech platforms inherently increases the risks of TFGBV, as engagement-driven algorithms, weak data protections, and content moderation rollbacks prioritize profit over user safety. Addressing TFGBV requires a fundamental shift away from the surveillance-based economy, stronger platform accountability measures, and regulatory frameworks that prioritize digital rights and gender justice over corporate interests.

That said, despite the risks of TFGBV, the digital space also serves as a critical tool for feminist activism, information access, and collective support. The Internet has enabled historically marginalized groups, including women and LGBTQIA+ communities, to organize, mobilize, and influence public discourse in ways that were previously inaccessible. Feminist movements across Latin America have effectively used digital platforms to advocate for reproductive rights, gender justice, and protections against gender-based violence, fostering transnational solidarity and amplifying feminist demands. Digital networks have also been crucial in documenting and resisting online gender-based violence, as organizations such as Derechos Digitales and feminist helplines in Bolivia, Brazil, and Ecuador provide digital security support, advocacy resources, and safe spaces for victims<sup>74</sup>.

## **15. What is the role of self-regulation of industry in addressing TFGBV and are there good practices in that regard?**

Tech companies have primarily relied on self-regulation to address TFGBV, but this approach has proven insufficient, inconsistent, and often harmful to victims. In fact, despite TFGBV being a structural issue rooted in the patriarchy and operating as a *continuum* from gender-based violence, some of its forms can be considered inherent risks from digital platforms’ business models.

---

<sup>73</sup> HUMAN RIGHTS CAMPAIGN. Meta’s New Policies: How They Endanger LGBTQ+ Communities and Our Tips for Staying Safe Online. 2025. <https://www.hrc.org/news/metas-new-policies-how-they-endanger-lgbtq-communities-and-our-tips-for-staying-safe-online>

<sup>74</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>



While some best practices have emerged, such as transparency reports, which provide data on abuse reports and content removals, these efforts remain voluntary and lack enforcement mechanisms. Advances in AI-driven content moderation have improved the detection of explicit or abusive material, yet algorithmic biases frequently result in over-policing feminist and activist content while allowing misogynistic abuse to persist<sup>75</sup>. Additionally, many platforms now offer user-controlled privacy features, such as blocking, filtering, and reporting tools, but their effectiveness is limited by inconsistent enforcement and the lack of meaningful redress for victims.

To address these systemic risks, binding international human rights-based reforms for the industry are urgently needed, going beyond self-regulation. Governments and regulatory bodies must require mandatory human rights impact assessments for tech companies, ensuring that platform design and moderation policies do not disproportionately harm marginalized groups. Faster and more transparent content removal mechanisms must be implemented for TFGBV-related reports, prioritizing survivor safety and due process.

Additionally, the creation of independent oversight bodies to audit platform moderation policies and algorithmic decision-making would increase transparency and accountability, preventing the misuse of digital spaces to silence and oppress vulnerable communities. Given Meta's recent changes in its content moderation policies and its lean towards authoritarianism and an anti-gender agenda, strengthening and assuring the independence of its oversight body becomes even more important. Without these structural changes, self-regulation will continue to serve as a shield for big techs - which have been highly and often unethically engaged against State regulations -, enabling the unchecked spread of TFGBV and reinforcing existing inequalities.

## **16. Are there established or promising good practices or new developments by industry, including regarding cooperation with civil society, academia or other stakeholders preventing or tackling TFGBV?**

One interesting multi-stakeholder initiative addressing TFGBV is the Coalition Against Stalkerware<sup>76</sup>, a collaboration between civil society, the private sector, and academia aimed at preventing and mitigating digital surveillance and abuse. Stalkerware—software designed to covertly monitor individuals' digital activities—is a growing tool of technology-facilitated intimate partner violence, disproportionately affecting women in abusive relationships.

The Coalition Against Stalkerware, launched in 2019, brings together cybersecurity companies, digital rights organizations, anti-domestic violence groups, and law enforcement to combat the development, distribution, and use of stalkerware. It focuses on three key areas: raising public awareness about the risks of stalkerware, improving technical solutions for detecting and preventing spyware, and enhancing survivor-centered responses by

---

<sup>75</sup> Wyer, S., Black, S. Algorithmic bias: sexualized violence against women in GPT-3 models. *AI Ethics* (2025). <https://doi.org/10.1007/s43681-024-00641-0>; UCL NEWS. Social media algorithms amplify misogynistic content to teens. 2024. <https://www.ucl.ac.uk/news/2024/feb/social-media-algorithms-amplify-misogynistic-content-teens>

<sup>76</sup> <https://stopstalkerware.org/>

providing resources to victims and training to support organizations. Notably, cybersecurity firms collaborate with civil society organizations to improve detection and removal of stalkerware from devices, while also pushing for stronger policy responses and industry accountability.

This coalition represents a good practice in cross-sector collaboration, as it demonstrates how tech companies, civil society, and researchers can work together to address TFGBV in a holistic way. By combining technical expertise, advocacy, and survivor support, the initiative has contributed to greater recognition of stalkerware as a digital threat, while also pressuring companies and governments to take stronger action against its use. This model of cooperation could serve as an example for broader efforts to combat TFGBV, particularly in areas such as platform accountability, AI-driven harassment, and gendered disinformation.

**17. Are there specific initiatives addressing TFGBV against certain groups of women and girls (including on the basis of personal or group characteristics, professional occupation or contextual factors) that you consider as good or promising practices or actions?**

Some initiatives that address TFGBV against certain groups of women and girls which deserve attention are:

- "Take Back the Tech!" campaign<sup>77</sup>: a global feminist initiative that provides digital self-defense strategies for women at risk
- Rede Transfeminista de Cuidados Digitais<sup>78</sup>: a network focused on strengthening the active participation of LGBTQIAPN+ people and other entities in the creation of technologies based on digital care
- Ciberseguras<sup>79</sup>: initiative that provides a series of materials in different formats and raises awareness on TFGBV and other cybersecurity and gender issues
- Some worldwide initiatives that protects and defend women's human rights and digital rights, such as:
  - The Rapid Response Fund of the Search for Common Ground<sup>80</sup>
  - Urgent Action Fund for Feminist<sup>81</sup>
  - Activism Coalition Against Online Violence<sup>82</sup>
  - Fondo de Acción Urgente Rapid Response Grants<sup>83</sup>

**18. Are there mechanisms or good practices on assessing the impact of new technology (at the development or functioning) on TFGBV (e.g. impact assessments)?**

---

<sup>77</sup> <https://www.takebackthetech.net/>

<sup>78</sup> <https://www.instagram.com/rtcuidadosdigitais/>

<sup>79</sup> <https://ciberseguras.org/>

<sup>80</sup> <https://www.sfcg.org/she-wins/rapid-response-fund/>

<sup>81</sup> <https://urgentactionfund.org/>

<sup>82</sup> <https://onlineviolenceresponsehub.org/>

<sup>83</sup> <https://fondoaccionurgente.org.co/en/what-we-do/rapid-response-grants/>

Implementing a moratorium or banning technologies that disproportionately affect human rights<sup>84</sup> and facilitate TFGBV is a good practice worth mentioning, as it prioritizes harm prevention and ensures that safeguards are in place before widespread deployment. Certain technologies, such as deepfake AI, have been extensively used to create non-consensual nudity content, disproportionately targeting women and marginalized groups. By imposing a temporary halt on such technologies, governments and institutions can assess their risks, establish accountability mechanisms, and develop legal frameworks that prevent abuse while allowing for ethical innovation.

For example, some countries have banned the sharing of deepfake pornography<sup>85</sup> due to its severe impact on victims, including reputational damage, emotional distress, and threats to personal safety. Similarly, facial recognition technology has faced moratoriums in several cities worldwide due to its potential for mass surveillance, discrimination, and misuse by abusers or authoritarian regimes<sup>86</sup>. By taking a precautionary approach, policymakers can ensure that new technologies do not exacerbate gender-based violence or reinforce systemic inequalities before they are introduced at scale.

## **19. Does your institution or organisation develop any practices, policies, campaigns or research relevant to understanding, preventing, raising awareness or tackling TFGBV?**

Yes, Derechos Digitales actively works on understanding, preventing, raising awareness, and tackling TFGBV through research, advocacy, support initiatives, and policy development, which includes the participation in global and regional governance spaces. Some key recent efforts include:

- Research and policy recommendations: Derechos Digitales collaborated with UNFPA to develop a guidance on rights-based law reform to address TFGBV, highlighting best practices for legislative and regulatory frameworks.
- Publications on TFGBV in Latin America<sup>87</sup> and towards a feminist approach to digital rights<sup>88</sup>.

---

<sup>84</sup> UN NEWS. 2019. Moratorium call on surveillance technology to end 'free-for-all' abuses: UN expert. <https://news.un.org/en/story/2019/06/1041231>

<sup>85</sup> ABC NEWS. Federal government to introduce ban on sharing of non-consensual deepfake pornography. 2024. <https://www.abc.net.au/news/2024-06-02/deepfake-pornography-sharing-image-based-abuse-criminal-prison/103923814>

<sup>86</sup> INNOVATION & TECH TODAY. 13 Cities Where Police Are Banned From Using Facial Recognition Tech. 2025. <https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/>

<sup>87</sup> DERECHOS DIGITALES. 2024. Helplines to address gender-based violence cases: Monitoring trends in Bolivia, Brazil and Ecuador. <https://www.derechosdigitales.org/wp-content/uploads/LineasAyuda-ENG-Portadillas-2.pdf>;

DERECHOS DIGITALES, APC. 2023. When Protection Becomes an Excuse for Criminalization: Gender considerations on cybercrime frameworks. [https://www.derechosdigitales.org/wp-content/uploads/gender\\_considerations\\_on\\_cybercrime.pdf](https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf)

<sup>88</sup> DERECHOS DIGITALES. Latin America in a Glimpse 2024: Reflections for a Community-Based, Feminist AI. [https://www.derechosdigitales.org/wp-content/uploads/Glimpse\\_2024\\_ENG.pdf](https://www.derechosdigitales.org/wp-content/uploads/Glimpse_2024_ENG.pdf)

- Campaigns to raise awareness: Derechos Digitales supports digital rights literacy initiatives, such as Navegando Libres por la Red<sup>89</sup>, which provides educational materials on online safety for women and marginalized communities.
- Presence in global and regional governance spaces: Derechos Digitales actively participated in governance discussions where gender was a central element, including the drafting and presentation of the Feminist Principles for Including Gender in the Global Digital Compact<sup>90</sup>. We also led civil society discussions on gender during the UN's debates on its Convention against Cybercrime.

## **20. Has your institution or organisation developed any practices, policies, campaigns or research relevant to supporting victims of TFGBV?**

Derechos Digitales is involved in several projects and partnerships that provide support to TFGBV victims. Some examples are:

- Helplines subject of Derechos Digitales' research which offer emotional support, legal guidance, and digital security assistance to TFGBV victims:
  - Centro S.O.S Digital (Bolivia)
  - Maria d'Ajuda (Brazil)
  - Navegando Libres por la Red (Ecuador)
- Regional initiatives that have been supported by the de Rapid Response Fund and the Digital Rights Fund, both managed by Derechos Digitales:
  - Hartas Mujeres – Online Feminism and Tech-Security Campaign for 16 Days of Activism, Chile, 2020
  - Coletiva Periféricas – COVID-19: Digital Gender Violence in Brazil During the Pandemic, Brazil, 2021
  - Mujeres con capacidad de soñar a colores – "Distanced, but not Disconnected": Women with Disabilities from the Guatemalan Highlands and the Right to Digital Participation in the Context of COVID-19, Guatemala, 2020
  - Corporación Promoción de la Mujer (TMC) – Network of Supporters Against Digital Gender Violence: Navigating Free, Ecuador, 2021
  - Universidade Livre Feminista – Navigating Together Through the Challenges of the Internet, Brazil, 2021
  - Universidade Livre Feminista – Navigating Together Through the Challenges of the Internet, Guatemala, 2021
  - Acuerpadas – Combative from the Networks, Nicaragua, 2022
  - Latfem – The Feminist Ecosystem of Latin America and the Caribbean in the Face of Digital Care: Ghosts, Obstacles, and Good Practices for Working in Safer Environments, Argentina, 2022
  - Cambio Sostenible – Digitally Secure, Colombia, 2022

<sup>89</sup> <https://navegandolibres.org/>

<sup>90</sup> APC. The Feminist Principles for including gender in the Global Digital Compact. 2023. <https://www.apc.org/en/pubs/feminist-principles-including-gender-global-digital-compact-0>

- Fundación Datos Protegidos – Support for Victims of Gender Violence and Digital Extortion, Chile, 2023
- Red Interuniversitaria Seguras y Educadas (RISE) – Techno-Feminists, Guatemala, 2022
- Asociación Illary – Green Tide and the Impact of Online Gender Violence in the Context of Mobilizations for the Decriminalization of Abortion in Ecuador (2019-2022), Ecuador, 2023
- CDD – Strengthening Cybersecurity for Catholic Feminists, Nicaragua, 2023
- Acción Feminista – Training Workshop for the Network of Facilitators in Digital Care Processes, Mexico, 2023
- Sursiendo – Technology, Gender, and Environment: Digital Campaign to Transform Technological Narratives Through the Voices of Affected Communities, Mexico, 2023
- Laboratorio Ciudadano – Protection and Support for Victims of Non-Consensual Dissemination of Intimate Images in Honduras, 2024
- Amaranta ONG – Research: Digital Vicarious Violence in Chile—Another Form of Technology-Facilitated Violence? Chile, 2024

**21. Are there specific good or promising civil society initiatives, campaigns or research addressing TFGBV against certain groups of women and girls (including on the basis of personal or group characteristics, professional occupation or contextual factors)?**

Besides the work being conducted by ourselves in Derechos Digitales, we recognize several other civil society initiatives as good practices in tackling TFGBV among specific groups of women and girls (some of them previously mentioned in this document already):

- Luchadoras MX (Mexico): a feminist collective that documents online violence cases and advocates for better digital protections for women activists.
- SocialTIC (Mexico): provides training on digital security and data protection for women journalists and human rights defenders.
- MariaLab (Brazil): focuses on digital safety for LGBTQIA+ individuals and women in vulnerable communities, offering privacy audits and cyber-resilience strategies.
- MonitorA (Brazil): a project designed to monitor political and electoral violence against female candidates on social media during elections.

**22. What work are you, your body or the OHCHR currently carrying out in the field of TFGBV and human rights? Please provide any relevant information such as links to reports, background material, sections or units involved, etc.**

N/A

**23. What are the gaps, if any, in the existing international human rights protection framework to address the impact of TFGBV? How could they be best addressed?**

As previously mentioned in this document, TFGBV violates a series of fundamental rights contained within the human rights framework. In this sense, even though not in a direct explicit way, the responsibility of States to address TFGBV derives from the existing human rights framework. The major gap in it is in relation to the private sector, especially companies holding technologies and digital platforms and services where TFGBV takes place.

In other words, there is an important lack of binding international mechanisms to hold technology companies accountable for human rights violations in general and TFGBV in particular. While international frameworks such as CEDAW, the UN Guiding Principles on Business and Human Rights, and various human rights treaties recognize gender-based violence as a human rights issue, there are no enforceable global standards that mandate big tech companies to prevent, mitigate, or remedy TFGBV on their platforms. This absence of oversight allows platforms to operate with impunity, prioritizing profit-driven engagement models over user safety and digital rights.

To address this gap, the international human rights system must move beyond voluntary guidelines and self-regulation by establishing binding obligations for digital platforms regarding TFGBV. This includes mandatory transparency and due diligence requirements, obligations to conduct human rights impact assessments, and accountability mechanisms that provide access to justice for survivors. Additionally, and guided by such international obligations, States can and should develop national regulatory frameworks that compel tech companies to take responsibility for algorithmic amplification of gendered abuse, weak moderation practices, and systemic failures in user protection. Without such mechanisms, the international human rights framework remains ineffective in addressing the growing role of digital platforms in enabling TFGBV.

**24. How could the current international human rights framework be best used or developed to address the impact and challenges of TFGBV with regard to the promotion and protection of all human rights?**

To effectively address TFGBV within the international human rights framework, it is essential to develop binding global standards that compel both states and tech companies to take responsibility for preventing and mitigating digital gender-based violence. One crucial step would be the creation of an international convention or protocol on TFGBV, which would require states to regulate TFGBV comprehensively, from a survivor-centric perspective and with a balanced approach. Such an instrument should establish clear mandates for platform transparency, ensure legal remedies for victims, prevention mechanisms and enforce stronger intersectional protections for marginalized groups.

Additionally, TFGBV protections must be mainstreamed into existing human rights treaties, including CEDAW, human rights conventions, and regional agreements, to explicitly recognize it as a gendered human rights issue. Expanding the scope of TFGBV protections

within international women's rights mechanisms would help close the gaps that leave survivors without effective redress.

Furthermore, big tech companies must be held accountable through enforceable obligations, such as global reporting requirements on how platforms handle TFGBV complaints and independent audits of content moderation practices to ensure transparency and effectiveness, which stem from frameworks such as the UN Business and Human Rights Principles. The same goes for the development of gender-sensitive technology impact assessments, which would help identify and mitigate risks of TFGBV before they escalate, making platforms safer and more equitable spaces.

A survivor-centered and intersectional approach must be prioritized in international law to address the specific vulnerabilities of women, LGBTQIA+ individuals, and other marginalized groups. At the same time, it is critical to ensure that freedom of expression and digital rights protections do not become barriers to combating TFGBV, which must be responded to through regulation and public policies drawn based on proportionality standards. By implementing these measures, the international human rights framework can evolve to provide meaningful protection against TFGBV while upholding fundamental rights.