SDG REPORT CARD

Technology-Facilitated Gender-Based Violence (TFGBV)

SDG 5.2 *Dr. Michaela Moura-Koçoğlu and Mary Adams*

US GRADE

C

Marginal Progress

The SDG Blind Spot

The United Nations Sustainable Development Goals (SDGs) are 17 non-binding global goals adopted in 2015 to address major social, economic, and environmental challenges by 2030. Under **SDG 5** on gender equality, **Indicator 5.1.1** tracks whether legal frameworks are in place to promote, enforce and monitor equality and non-discrimination on the basis of sex; and **Indicators 5.2.1 and 5.2.2** track the proportion of women and girls subject to physical, sexual, or psychological violence by an intimate partner and by persons other than an intimate partner (UN Statistics Division 2026). **No SDG indicator was designed to capture technology-facilitated gender-based violence** (TFGBV), and there is no agreed intergovernmental definition.

The unfortunate result is that **no country to date reports TFGBV data under SDG Target 5.2,** exposing a gap: Indicators 5.2.1 and 5.2.2 record no digital tactics, and the legal frameworks 5.1.1 monitors were not built to treat TFGBV as a form of gender violence requiring protection (Baekgaard 2024).

Compared with emerging international approaches, U.S. monitoring of technology-facilitated gender-based violence remains relatively fragmented (EU 2026). Federal surveys capture important forms of technology-facilitated sexual violence and stalking, but the **U.S. lacks a comprehensive national system for measuring the broader range of TFGBV.** Nonetheless, closing the gaps in measuring TFGBV under Target 5.2 is within direct reach of the US Congress.

TFGBV Silences Women's Voices

Technology-facilitated gender-based violence undermines women's safety, privacy, health, and equal participation in digital life, with political, social, and economic consequences that are particularly acute for marginalized women and girls (UN Women 2025a).

> *In 2021, 23-year-old politician Sabrina Javellana fell victim to **AI deepfake pornography**, resulting in her withdrawal from politics: "I felt fear for my family, my home," she said. "It impacted my stress, my health, everything. It crushed me to step away, but I had to for my sanity, for my survival, for my health, for my safety" (The Independent 2026).*

Technology-facilitated tactics clearly affect women's safety: GPS tracking, stalkerware, and social media monitoring affected **16-29%** of stalking victims; **46.8%** received **unwanted social-media messages**; **36.3%** were **tracked online** without consent (CDC 2025). TFGBV silences women's voices and weakens their equal participation in democratic decision-making in the United States.

No International Legal Definition of TFGBV

TFGBV lacks an agreed definition at the United Nations, as it emerged from feminist research and advocacy rather than intergovernmental process. The most widely used definition recognizes TFGBV as any act "committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms" (UN Women 2023). TFGBV may include cyberstalking, non-consensual distribution of intimate images, image-based abuse ("deepfakes"), sextortion, doxing, and stalkerware-enabled coercive control (UN Women 2025b).

99%

of nonconsensual **sexually explicit deepfakes** target women

UN Women 2026

24.2%

of US respondents have experienced **image-based sexual abuse**.

Only 38.8% reported to any agency; 30.9% disclosed to no one.

Umbach et al. 2025

22.5%

of US women (28.8 million) have experienced **stalking** in their lifetime.

State-level prevalence ranges from 15-35%.

CDC 2025

16-29%

of stalking victims

were affected by tech-facilitated tactics such as GPS tracking, stalkerware, and social media monitoring.

46.8% received unwanted social media messages; 36.6% were tracked online without consent.

CDC 2025

Data Gap in the United States

The United States measures some forms of technology-facilitated sexual violence and stalking but not the full scope of TFGBV (US Congress 2022). Although international research shows elevated online abuse against Black and racialized women as well as women with disabilities, **no federal source disaggregates TFGBV data by race, disability, or immigration status** (Amnesty International 2018).

- The **2022 VAWA reauthorization** added the term '**technological abuse**' for conduct intended to harm, threaten, intimidate, control, stalk, harass, impersonate, exploit, extort, or monitor another person through any form of technology but did not mention **intimate partnerships** which indicator 5.2.2 measures (US Code 2022).
- The 2025 **TAKE IT DOWN Act** makes it a federal **crime to share nonconsensual intimate images** (NCII), including AI-generated fakes, and requires platforms to remove reported content within 48 hours (US Congress 2025). However, it **does not regulate AI "nudification" tools** themselves, nor provide federal resources to detect, investigate, and prevent these crimes (Fichtner et al. 2026).
- The bipartisan **DEFIANCE Act**, which would extend the NCII law to intimate digital forgeries and other matters, passed the Senate by unanimous consent on January 13, 2026, and **awaits House action** (US Congress 2026).

> ***No Federal Law Makes Doxing a Crime:*** Existing law protects only certain federal workers (US Code 2024). State laws vary widely: only 17 states have specific doxing laws, and definitions and enforcement differ from state to state (Council of State Governments 2025).

The only 24/7 helpline
for image-based sexual abuse
is operated by an NGO
the Cyber Civil Rights Initiative
under federal grants.

No comparable service exists for cyberstalking, doxing, or stalkerware-enabled coercive control.

CCRI 2026

Cyberstalking
requires proof of specific intent to harass, intimidate, or injure.

It fails to capture covert tactics such as stalkerware monitoring, often hidden for months.

US Code 1996

US Women's Caucus Recommendations

Adopt a standardized federal definition and taxonomy of TFGBV
and fund validated, disaggregated data collection using existing federal instruments.

Develop a standardized TFGBV module
for federal surveys that captures gendered tactics, with results disaggregated by race, disability, and immigration status.

Recognize TFGBV as a covered form of gender-based violence
in victim-services programs to close eligibility gaps for survivors of non-intimate-partner relationships.

References

Amnesty International 2018. *Twitter study reveals shocking scale of online abuse against women.* The study found Black women 84% more likely to appear in abusive tweets.
Baekgaard 2024. *Technology-Facilitated Gender-Based Violence: An Emerging Issue in Women, Peace, and Security.*
CCRI 2026. *CCRI Crisis Helpline.* Funded by Department of Justice Office for Victims of Crime.
CDC 2025. *The National Intimate Partner and Sexual Violence Survey (NISVS): 2023/2024 Stalking Data Brief.* Sharon G. Smith et al.
Council of State Governments 2025. *Doxing: State Protections Against Digital Threats.*
EU 2026. *EU Gender-based Violence Survey: Evidence for Policy and Practice.*
Fichtner et al. 2026. *Criminalizing Deepfakes: A Comprehensive Review of US Legislative Responses to Synthetic Media Abuse.*
The Independent 2026. *"Slap in the face": Victim of AI deepfake attack shreds House stonewalling of AOC's anti-abuse bill.* Rhian Lubin and Eric Garcia.
Umbach et al. 2025. *Prevalence and impacts of image-based sexual abuse victimization: A multinational study.*
UN Statistics Division 2026. *SDG Indicators: Metadata Repository.*
UN Women 2023. *Technology-facilitated Violence against Women: Towards a Common Definition.*
UN Women 2025a. *UN Women Strategy: Preventing and Eliminating Technology-Facilitated Violence Against Women and Girls.*
UN Women 2025b. *FAQ: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women and girls.*
UN Women 2026. *When justice fails: Why women can't get protection from AI deepfake abuse.*
US Code 1996. 18 U.S.C. § 2261A. Interstate Stalking Punishment and Prevention Act.
US Code 2022. 34 U.S.C. § 12291(a)(40); 15 U.S.C. § 6851.
US Code 2024. 18 U.S.C. §119. *Protection of individuals performing certain official duties.*
US Congress 2022. *S.2629 - Better Cybercrime Metrics Act.* Covers digital identity theft and stalking, but not sextortion, doxing, or other harms.
US Congress 2025. *S.146 - TAKE IT DOWN Act.* Pub. L. 119-12 (May 19, 2025), codified at 47 U.S.C. §§ 223(h) and 223a.
US Congress 2026. *S.1837 - DEFIANCE Act of 2025.* Passed the Senate by unanimous consent January 13, 2026; held at the House desk.