

ARTICLE 4 - Published on the EPALE Platform on 19th July 2025

<https://epale.ec.europa.eu/en/content/unmasking-gender-based-technology-driven-violence-gbtdv>

Unmasking Gender-Based Technology-Driven Violence (GBTDV)

The fight against Gender-Based Technology-Driven Violence (GBTDV) is an ongoing struggle that demands continuous innovation and advocacy. While digital spaces provide significant opportunities, they also serve as breeding grounds for new types of harm. GBTDV is a widespread problem that targets individuals based on their gender through digital channels.

GBTDV encompasses a range of harmful acts, including online harassment, cyberstalking, the non-consensual sharing of intimate images (often termed "revenge porn"), deepfake pornography, and doxxing (the public release of private information without consent). These acts are not merely isolated incidents but are often rooted in broader societal issues like misogyny, discrimination, and power imbalances, amplified by the anonymity and reach of digital platforms.

Recent data from Amnesty International (2024) indicates that 38% of women who spend time online have been the target of online violence, and 85% have witnessed it. New polling commissioned by Amnesty International UK (March 2025) reveals that 44% of Gen Z women in the UK who experienced online misogyny reported negative mental health impacts. This research also found that 73% of Gen Z social media users have witnessed misogynistic content online, with half encountering it weekly.

Fortifying Defenses: Prevention and Response Strategies

Combating GBTDV requires a multi-faceted approach, encompassing digital security measures, community awareness, platform accountability, and robust legal frameworks.

Digital Security and Literacy: Empowering Individuals. Individual empowerment through digital literacy is a crucial first line of defense. This involves:

- **Strong Passwords and Two-Factor Authentication (2FA):** Implementing complex, unique passwords for all online accounts and enabling 2FA adds a critical layer of security, making it significantly harder for unauthorized individuals to gain access.
- **Privacy Settings Vigilance:** Regularly reviewing and adjusting privacy settings on social media and other online platforms can limit the visibility of personal information and prevent unwanted contact.

- **Mindful Information Sharing:** Exercising caution about the personal information shared online, even with trusted connections, can reduce vulnerability to doxxing and other forms of digital harm.

Beyond individual actions, fostering community awareness and digital literacy is paramount. Workshops and training programs in schools, workplaces, and communities can educate individuals on recognizing the signs of online violence and equip them with strategies for addressing it. Bystander intervention programs are also vital, encouraging safe and effective intervention when witnessing GBTDV.

Platform Accountability: Shifting the Burden While individual responsibility is important, the onus also lies heavily on technology companies to create safer digital environments. This requires:

- **Stricter Content Moderation:** Tech companies must enforce more stringent policies regarding abusive content and invest in robust content moderation systems.
- **Transparency in Reporting:** Reporting mechanisms for abusive content need to be transparent, accessible, and efficient, ensuring that victims' complaints are addressed promptly and effectively.
- **AI Tools for Detection:** Encouraging the development and deployment of AI tools to proactively detect and remove harmful content, including hate speech, deepfakes, and non-consensual images, can significantly mitigate the spread of GBTDV. However, it's crucial that these AI models are trained on diverse datasets to avoid biases and ensure accuracy.

Immediate Steps for Victims: Taking Back Control For those who experience GBTDV, immediate action can be critical in mitigating harm and seeking justice:

- **Document Everything:** Preserving evidence is paramount. Screenshots, emails, message logs, and any other relevant digital traces should be meticulously saved. This documentation is crucial for legal action or platform-based reporting.
- **Report the Abuse:** Utilizing in-platform reporting mechanisms on social media platforms (e.g., Facebook, X, Instagram) is often the first step.
- **Seek Legal Action:** Many countries have enacted cybercrime laws that provide legal recourse against digital abuse. Consulting with legal professionals can help victims understand their rights and options.

Global Efforts: Legal Protections and Policy Frameworks

Governments and international bodies are increasingly recognizing the severity of GBTDV and implementing legal and policy frameworks to combat it.

Legal Protections Across Borders

- **European Union:** The General Data Protection Regulation (GDPR) offers robust data privacy protections that can be leveraged in cases of GBTDV involving the misuse of personal data. Furthermore, the EU's Digital Services Act (DSA), which came into full effect in February 2024, mandates stricter rules for online platforms regarding content moderation and transparency, directly impacting how tech companies address harmful content, including GBTDV. In January 2025, major tech companies agreed to enhance efforts against online hate speech under a revised code of conduct integrated with the DSA, mandating collaboration with non-profit organizations and requiring companies to review at least two-thirds of reported incidents within 24 hours. Additionally, in October 2024, the EU established a framework to impose sanctions on individuals and entities responsible for cyberattacks, misinformation, and sabotage.
- **United States:** The Violence Against Women Act (VAWA) includes provisions that address cyber harassment and other forms of technology-facilitated abuse.
- **India:** The Information Technology Act (2000) criminalizes cyberstalking and various forms of online abuse.
- **Serbia:** The United Nations Population Fund (UNFPA) launched the "Bodyright Campaign" in November 2022 to raise awareness about technology-facilitated gender-based violence (TFGBV), highlighting that 85% of women globally have experienced or witnessed online violence. The UN in Serbia also collaborated with the Judicial Academy to develop an online learning platform for legal professionals on domestic violence prevention, including technology-facilitated abuse.
- **Japan:** In June 2022, Japan's parliament passed legislation making "online insults" punishable by imprisonment, with offenders facing up to one year in prison or fines. This legislative change was influenced by tragic cases of cyberbullying, including the suicide of reality TV star Hana Kimura in 2020.

Mental Health and Support Resources: Healing and Recovery

Beyond legal and technical measures, access to mental health and support resources is crucial for victims. Organizations like the Cyber Civil Rights Initiative (CCRI) offer vital support, and online therapy and support groups provide safe spaces for healing and recovery.

The Role of Technology and Advocacy in a Safer Digital Future

Technology itself, while a vector for harm, can also be a powerful tool for protection.

Encouraging Gender-Sensitive Digital Policies in Companies Many social media and tech companies have historically had inadequate policies for addressing gendered digital violence. However, advocacy efforts have led to some positive changes:

- **Facebook/Meta:** Has introduced AI-powered automated detection for hate speech and abuse targeting women.
- **X (formerly Twitter):** Following significant backlash over online abuse, third-party apps like Block Party have emerged to help users filter out harassment.
- **Instagram:** Improved comment filtering in 2022 to automatically hide abusive language.

Despite these advancements, challenges remain. Many AI models struggle to recognize context, leading to false positives or the overlooking of abuse. Continued advocacy is needed to push companies to invest in better AI training datasets and to prioritize human moderators trained in gender-based violence. Faster response times to abuse complaints and stricter penalties for repeated offenders, such as permanent bans, are also critical demands.

Digital Self-Defense Tools for Online Safety A growing number of tools are available to help individuals protect themselves:

- **Block Party (for X):** Helps users block harassers and filter toxic messages.
- **Face Guardian:** An AI tool designed to detect deepfake pornographic images and alert potential victims.
- **StopNCII.org:** A vital resource for victims of non-consensual intimate image abuse, assisting in the removal of their photos from the internet.
- **Privacy Badger:** A browser extension that blocks trackers from collecting personal data.

Promoting awareness and integration of these tools through cybersecurity training in schools and workplaces, and encouraging tech companies to integrate them into their platforms by default, can significantly enhance online safety for everyone.

In conclusion, GBTDV is a complex and evolving threat that demands a comprehensive and collaborative response. By understanding its various forms, implementing robust prevention and response strategies, strengthening legal frameworks, and leveraging technological

advancements, we can collectively work towards creating a digital world that is safer, more equitable, and free from gender-based violence. The journey is ongoing, but with sustained effort and commitment, a future where digital spaces are truly empowering for all is within reach.

👉 The Erasmus MEDEA project: Developing Media Literacy to debunk gender-related media manipulation and fake news n. 2024-1-LV01-KA210-ADU-000243248 - deals with these topics. To learn more, visit the Facebook page and the project website to access the Media Literacy Toolkit and utilize its contents.

👉 For more information about the MEDEA project and to access the Toolkit, visit <https://www.facebook.com/MedeaErasmusProject> and <https://www.jelgavaszoninklubs.lv/projects/>

References

- Amnesty International. (2020). *Troll Patrol: A global study of online abuse against women*.
- AP News. (2025, March). *Italy approves draft law defining 'femicide' in penal code*.
- AP News. (2025, October). *EU establishes a sanctions system for cyberattacks and foreign interference*.
- European Commission. (2024, February 17). *Digital Services Act: Commission welcomes the start of application for all online platforms*.
- EST - European Student Think Tank. (2025). *Italy's legal reforms against revenge porn*.
- euronews. (2025, July). *Romania amends domestic violence legislation to include 'cybernetic violence'*.
- GLAAD. (2022). *Accelerating acceptance: A survey of LGBTQ+ Americans*.
- Indiatimes. (2025, June). *Japan makes online insults punishable by imprisonment*.
- Medium. (2025, June). *Japan's new law targets online insults after Hana Kimura's death*.
- Reuters. (2025, January). *Tech giants agree to stricter EU code against online hate speech*.
- Reuters, The Guardian, AP News. (2025). *Giulia Cecchetti Foundation promotes education against gender-based violence*.
- UN Women. (2021). *Measuring the shadow pandemic: Violence against women during COVID-19*.
- UN Sustainable Development Goals, The United Nations in Serbia. (n.d.). *Digital Education for Legal Professionals*.
- The United Nations in Serbia. (2025, November). *Bodyright Campaign raises awareness on technology-facilitated gender-based violence*.

Literature Sources

- Amnesty International. (Ongoing). *Reports and campaigns on online violence and digital rights*.

- Council of Europe. (Ongoing). *Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)*.
- European Commission. (Ongoing). *Digital Services Act (DSA) and other digital policy initiatives*.
- GLAAD. (Ongoing). *Research and advocacy on LGBTQ+ representation and safety in media*.
- Human Rights Watch. (Ongoing). *Reports on digital rights, online harassment, and gender-based violence*.
- NCMEC (National Center for Missing and Exploited Children). (Ongoing). *Resources and support for victims of online child exploitation and abuse*.
- Pew Research Center. (Ongoing). *Studies on online harassment and digital behavior*.
- UN Women. (Ongoing). *Publications and initiatives on ending violence against women and girls*.
- United Nations. (Ongoing). *Reports and resolutions on human rights in the digital age*.
- Women's Rights Organizations (e.g., Equality Now, Women's Aid). (Ongoing). *Advocacy and support for victims of gender-based violence*.