

Building Resilience Against Human Security Threats and Risks: From Best Practices to Strategies

Frederic Labarre, Elena Mandalenakis, George Niculescu (Eds.)

Study Group Information



UNSER HEER

Gender-Based Online Violence in Moldova, Ukraine and Georgia

Sanda Sandu, Elena Mârzac

Introduction

The ongoing challenges such as pushback against gender equality and the effects of conflicts like the war in Ukraine and military tensions in the Armenia-Azerbaijan border region have made addressing harmful gender stereotypes more critical than ever. Russia's full-scale invasion of Ukraine has resulted in the largest humanitarian crisis in Europe since World War II, with grave consequences for women and girls. Nearly 8 million refugees have fled Ukraine, and an estimated 5.4 million people are internally displaced, with women constituting 90% of those who have fled the country. The additional burden of caregiving responsibilities, exacerbated by the war and compounded by the adversities of the COVID-19 pandemic, further exacerbates gender disparities.¹ The internet has increasingly become a space where gendered hostilities are pronounced and proliferated, ranging from unsolicited explicit content and cyberstalking to more covert forms of harassment. According to a report by the United Nations, women are 27 times more likely to be harassed online, highlighting the pervasive nature of this issue across diverse demographics and geographic locations. Online harassment perpetuates gender inequities and stifles voices, contributing to broader societal repercussions. These include restrictions on freedom of expression, detrimental effects on mental health, and barriers to economic opportunities for women, underscoring the urgent need for concerted action to address this multifaceted challenge.

These issues are indeed pressing and require immediate attention and action from all sectors of society. Moreover, today's digital age, online platforms

¹ United Nations, "Women Are Increasingly At-Risk in Conflict, Underrepresented in Peace Processes, according to UN Secretary-General Report" *UN Women – Headquarters* (October 24, 2023), <https://www.unwomen.org/en/news-stories/feature-story/2023/10/women-are-increasingly-at-risk-in-conflict-underrepresented-in-peace-processes-according-to-un-secretary-general-report>.

serve as a modern agora; a space where people engage, exchange ideas, and build communities. However, like any public space, online platforms also reflect the shadows of societal issues: they provide ways of expressing covert societal tendencies, divisions, and behaviours such as online violence. This has emerged as a troubling by-product of the digital evolution, often mirroring the systemic prejudices and inequalities entrenched in offline realms. A particularly distressing facet of this is the prevalence of gender-based online violence.

Taking into consideration the existing context, this article will examine gender-based online violence in Eastern Europe, particularly in Moldova, Ukraine, and Georgia, with the aim of understanding the unique challenges individuals face in these regions. It assesses the role and response of major social media platforms in addressing these challenges and advocates for a human rights-based approach to combat such violence in the digital domain. By reviewing current research and international human rights instruments, the article emphasises the importance of privacy, freedom from violence, and the commitment of state and regional actors to address risks and ensure rights implementation. It argues that adopting a human rights perspective on technology-based violence is crucial for holding both State and non-State actors accountable and proposes recommendations to create a safer and more inclusive online environment. Through insightful analysis and recommendations, the article contributes to the discourse on technology-driven gender-based violence and underscores the necessity of a rights-based framework for effective intervention and accountability.

Gender-based violence (GBV) is an umbrella term for harmful acts of abuse perpetrated against a person's will and rooted in a system of unequal power between women and men. This is true for both conflict-affected and non-conflict settings.²

Online gender-based violence³ stems from misogyny in physical spaces and the cultural norms that shape our lives. Traditional forms of gender-based

² International Rescue Committee, *The IRC in the EU*, IRC, (November 23, 2022), https://www.rescue.org/eu/article/what-gender-based-violence-and-how-do-we-prevent-it?gad_source=1.

³ UN Women, "Frequently Asked Questions: Tech-Facilitated Gender-Based Violence."

violence, like intimate partner violence, street harassment, and rape, which are well-documented in the context of violence against women, have given rise to their online counterparts. The emergence of online gender-based violence is also influenced by the practices of online communities and the absence of regulations addressing gender-specific harassment and violence within these communities.

Certain groups, notably women in professions with a prominent online presence such as leaders, politicians, artists, journalists, and advocates for human rights and gender equality, become particularly susceptible targets for coordinated campaigns of online gendered disinformation, harassment, hate speech, and even threats of death and rape.

Research suggests that the *modus operandi* of social media platforms amplify gendered disinformation and hate speech with devastating effects on women's lives in diverse ways. Women can be professionally and reputationally damaged, leading them to censor or self-censor, discouraging them from entering specific professional fields with public exposure and their mental health can be highly affected.⁴

From unsolicited explicit content and cyberstalking to more covert forms of harassment, the internet has increasingly become a space where gendered hostilities are both pronounced and proliferated. The United Nations has recognized this phenomenon, noting that women are 27 times more likely to be harassed online.⁵ This statistic transcends and cuts through societal and economic boundaries, encompassing women from all walks of life and from every corner of the globe.

The intersection of online violence with gender is more than just a digital safety issue – it strikes at the core of human rights and human security. Every

UN Women – Headquarters n.d. <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence>.

⁴ UNESCO, “How to Combat Hate Speech and Gendered Disinformation Online? UNESCO Provides Some Ideas” (2023), <https://www.unesco.org/en/articles/how-combat-hate-speech-and-gendered-disinformation-online-unesco-provides-some-ideas>.

⁵ UN Women, “Creating Safe Digital Spaces free of Trolls, Doxing and Hate Speech”, (November 2023), <https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech>.

individual has the inherent right to live without fear, express themselves without retaliation, and participate in digital spaces without facing threats based on their gender.

From a human security perspective, the pervasive nature of gender-based online violence threatens the fundamental pillars of personal security. These virtual threats often transcend to the physical world with consequences in mental health, social relationships, and even physical safety.

The contemporary issue of gender-based violence is a major human rights and equality issue that concerns all physical, sexual and psychological harm to women and girls. Although, gender-based violence affects both men and women, violence against women and girls is one of the most prevalent violations of human rights in the world. Worldwide, it is estimated that 1 in 3 women will experience some form of physical or sexual abuse in their lifetime.⁶

Addressing online gender-based violence (GBV) requires widespread social change. In this article, our focus is on the GBV that is mediated, practiced, or amplified via Internet technologies. Online GBV includes a broad range of behaviors facilitated through various digital technologies. Different types of intermediaries have different levels of involvement – and therefore different responsibilities – concerning different types of GBV.⁷

Tech platforms play a pivotal role in this discourse. Serving as the gatekeepers of modern communication, they bear a significant responsibility. Their policies, algorithms, and community standards can either amplify or mitigate these issues. Addressing gender-based online violence is not just a corporate responsibility for them – it's a matter of upholding human rights in the digital era.

⁶ Lauren Granger, “Tackling gender-based violence using the human rights-based approach to development”, Sheffield University, n.d. <https://www.sheffield.ac.uk/geography/news/tackling-gender-based-violence-using-human-rights-based-approach-development>.

⁷ N. Suzor, M. Dragiewicz, B. Harris, et al, “Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online”, <https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.185>.

Human Rights Framework

The concept of human rights is predicated upon the fundamental idea that every individual, irrespective of race, gender, nationality, or faith, is entitled to a set of inalienable rights simply by virtue of being human. These rights serve as the bedrock upon which individuals can lead lives of dignity, freedom, and equality.

Within the digital sphere, the Universal Declaration of Human Rights (UDHR) sets a precedent. Article 19, for instance, accentuates the right to freedom of expression, encompassing the freedom “to seek, receive, and impart information and ideas through any media and regardless of frontiers.”⁸ In essence, this underscores the right to digital access and expression. The digital realm also amplifies the importance of other rights, such as the right to privacy (Article 12) and the prohibition of discrimination (Article 7). As such, the online world is not a separate entity, but an extension of the physical world wherein human rights must be respected and upheld.

Human Security

Initially emerging post-Cold War, human security shifted the focus from state security to that of the individual, arguing for a more holistic approach to threats and challenges. It comprises various dimensions, including economic, food, health, environmental, personal, community, and political security. The idea is to emphasise the “freedom from want” and “freedom from fear” for every individual.

Human security is people-centred, not threat-centred. Human security is a condition that results from an effective political, economic, social, cultural, and natural environment. But to uphold human security effectively, a pro-active attitude towards threats – whether they are threats from natural disasters such as an earthquake or the ongoing threats faced by the destitute – is essential.⁹

⁸ The Universal Declaration of Human Rights (UDHR) was proclaimed by the United Nations General Assembly in Paris on 10 December 1948 (General Assembly resolution 217 A) see <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

⁹ Sabina Alkire, “A Conceptual Framework for Human Security”, Oxford University, (2003). <https://ora.ox.ac.uk/objects/uuid:d2907237-2a9f-4ce5-a403-a6254020052d>.

In the context of online spaces, human security translates to an environment where users are free from digital threats that could compromise their well-being, whether those threats are data breaches, cyberbullying, or disinformation campaigns. The virtual realm, with its global connectivity, blurs the lines of traditional threats, making the need for human security even more salient. Through policy discussions and case studies, experts can derive general frameworks and guiding principles for future interventions.¹⁰ Digital platforms, thus, need to ensure a protective environment that safeguards the psychological, social, and sometimes physical well-being of its users. Online gender-based violence can manifest through different methods, encompassing activities like tracking and surveillance, hacking, spamming, and the malicious sharing of intimate messages and photos.

Gender-Based Online Violence

Gender-based online violence can be defined as any act perpetrated against a person's will, having a harmful or negative effect on the individual, and is determined or influenced by their gender. In online settings, this manifests in various forms:

- **Cyberstalking:** Persistent online harassment, often resulting in the victim fearing for their safety.
- **Harassment:** includes acts that use information and communications technology in terrorizing and intimidating victims through physical, psychological, and emotional threats, unwanted sexual misogynistic, transphobic, homophobic and sexist remarks and comments online whether publicly or in direct messages.¹¹
- **Non-consensual distribution of intimate content:** Also known as “revenge porn,” where explicit images or videos are shared without the depicted person's consent.
- **Trolling and Hate Speech:** Targeted online attacks, often on social media, based on a person's gender or gender identity.

¹⁰ Mark Latonero, and Zachary Gold “Data, human rights & human security”, *Human Rights & Human Security* (July 1, 2015).

¹¹ UN Women, “Tech-Facilitated Gender-Based Violence.” UN Women – Headquarters, n. d. <https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/tech-facilitated-gender-based-violence>.

- **Doxxing:** Publicly revealing private information about an individual without their consent, which is especially harmful when used as a tool of gender-based intimidation.

The complexity of human rights that are violated due to the gender-based online violence includes – the right to security of a person (UDHR 3), to access to information (UDHR 19), to take part in government (UDHR 21), to be free from unlawful attacks on one’s honour and reputation (ICCPR 17), and to truth (Resolution 2005/66).

Harassment can take many forms, including gendered attacks on volunteers who either publicly identify as female, transgender, or non-binary, doxing of personal information as well as threats of violence. At its most fundamental level, online harassment can impact on the right to be treated with dignity, but it can also impact on the right to: non-discrimination, right to security of persons (UDHR 3), privacy (UDHR 12), expression (UDHR 19), assembly (UDHR 20), participation in cultural life (UDHR 27), and the right to be free from unlawful attacks on one’s honour and reputation (ICCPR 17).

Government Surveillance and Censorship

Human rights are being challenged around the world, especially in relation to free expression, freedom of the press, internet blackouts, internet content controls, and crackdowns on human rights defenders. For internet users these infringements may impact on the rights to security of persons (UDHR 3), to be free from torture (UDHR 5), privacy (UDHR 12), expression (UDHR 19), assembly (UDHR 20) and to take part in government (UDHR 21). The following risks can be manifested:

- Online surveillance – especially in countries with restricted internet freedoms or authoritarian governments and on topics considered taboo in those countries;
- Requests for user data, including formal and informal government requests to the Internet Platforms, handle non-public data to receive requests directly from government officials;
- Government censorship, ranging from blocking certain websites or articles.

The implications of such actions are profound. Victims often experience psychological trauma, which can escalate to physical threats in some instances. Gender-based online violence not only infringes upon the rights of individuals to live without fear but also poses a significant barrier to their full and meaningful participation in the digital world. It challenges the very tenets of human rights and security, pushing the narrative towards urgent and substantial action against this digital scourge.

Regional Context

Eastern Europe, with its rich tapestry of cultures, histories, and socio-political intricacies, presents a unique tableau when discussing digital rights and online behaviours. Although gender equality in Eastern Europe – Georgia, Moldova, and Ukraine – is formally enshrined in the countries’ constitutions and legal systems, the lack of gender mainstreaming inhibits substantive gender equality.¹² The societal acceptance of norms that are deemed ‘misogynistic’ has a large impact on the prevalence of gender-based violence online. Cultural norms and beliefs are carried from physical communities into online spaces by actors who engage in this behaviour in person or who already agree with misogynist ideas. People who engage in physical violence against women also are likely to engage in online forms of violence. Through cultural causes, scholars claim that rather than technology creating violence online, it simply provides a new platform which users adapt to suit their desired action, some of which may include acts such as doxing, threatening, or stalking women.

Gender Rights

Over the years, Eastern Europe has seen a progressive shift in acknowledging and legislating for gender rights. Some countries have made notable strides, ratifying international conventions like the Istanbul Convention (aimed at preventing and combating violence against women), while others grapple with resistance from conservative factions.

¹² “Bringing Together Civil Society in the EU’s Neighbouring Countries in the Name of Gender Equality”, Niras, (2022), <https://www.niras.com/news/bringing-together-civil-society-in-the-eu-s-neighbouring-countries-in-the-name-of-gender-equality/>.

- The Council of Europe Convention on preventing and combating violence against women and domestic violence (the Istanbul Convention) was ratified on 19 May 2017 by Georgia.¹³
- The Istanbul Convention was also ratified by the Republic of Moldova and entered into force on 1 May 2022.¹⁴
- On 1 November, after approval by the Ukrainian Parliament on 20 June 2022 and ratification of the Istanbul Convention on 18 July 2022.¹⁵

Digital Infrastructure and Gender Rights

The region has witnessed rapid digitization over the past two decades. Internet penetration rates have surged. However, disparities exist. While urban areas boast high-speed connectivity and tech literacy, rural areas often lag,

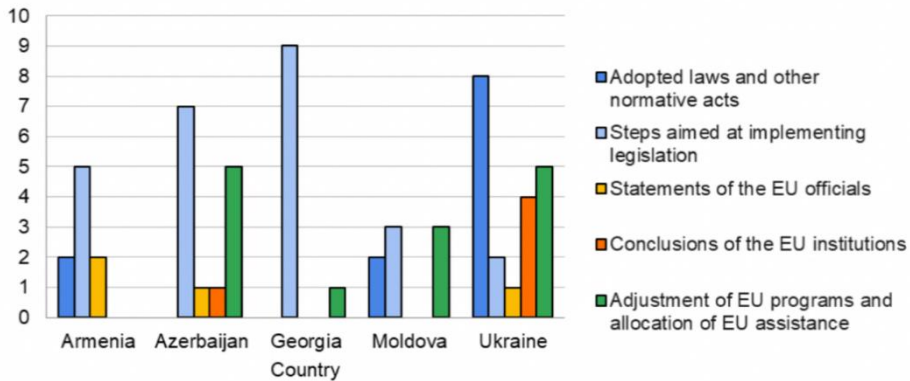


Figure 1: “Together for Resilient Digital Transformation”¹⁶

¹³ Council of Europe, “Georgia – Istanbul Convention Action against Violence against Women and Domestic Violence”, (2014), <https://www.coe.int/en/web/istanbul-convention/georgia>.

¹⁴ Council of Europe, “The Republic of Moldova Ratifies the Istanbul Convention”, *Istanbul Convention Action against Violence against Women and Domestic Violence* (January 31, 2022), <https://www.coe.int/en/web/istanbul-convention/-/the-republic-of-moldova-ratifies-the-istanbul-convention>.

¹⁵ “The Istanbul Convention Entered into Force on 1 November 2022 – Council of Europe Office in Ukraine”, *Council of Europe Office in Ukraine*, n.d. <https://www.coe.int/en/web/kyiv/-/the-istanbul-convention-entered-into-force-on-1-november-2022>.



¹⁶ Maksym Koriavets, “Resilient digital transformation in the Eastern Partnership region: State of play in 2022 and recommendations”, *Civil Society Organization “Polissya Foundation*

leading to a digital divide. Priority steps for the Republic of Moldova are also aiming at improving connectivity by anchoring Moldova in the TEN-T network. Digital flagship Initiatives for Georgia suggest developing high-speed broadband infrastructure for rural settlements. The Ukrainian flagship agenda primarily focuses on accelerating digital transformation through the modernization of public IT infrastructure.

Internet Freedom

Freedom House assesses the level of internet freedom in 70 countries around the world through its annual Freedom on the Net report. According to Freedom House, Georgians are generally free to express themselves online without fear of legal penalties, but several prosecutions for online activity have raised concerns in the past. The authorities periodically investigate internet users who threaten online, and civil society groups say their response can be disproportionate.¹⁷

In 2017, the Parliament of Georgia adopted new surveillance regulations after the Constitutional Court struck down previous surveillance legislation in 2016, which had forced companies to retain user metadata for two years and allowed authorities real-time access to vast amounts of user data.¹⁸

Country 	Total Score and Status	Obstacles to Access	Limits on Content	Violations of User Rights
Georgia	78  Free	19	31	28

Scores are based on a scale of 0 (least free) to 100 (most free)

* Indicates a territory as opposed to an independent country.

Table 1: Freedom House Score for Georgia

for International and Regional Studies”.

¹⁷ “Georgia: Freedom on the Net 2022 Country Report”, Freedom House (2022). <https://freedomhouse.org/country/georgia/freedom-net/2022>.

¹⁸ Public Defender (Ombudsman) of Georgia, “Constitutional Claim regarding Georgian Law ‘On Electronic Communications’”, (February 2, 2014), <https://ombudsman.ge/eng/konstitutsiuri-sarchelebi/constitutional-claim-regarding-georgian-law-on-electronic-communications>.

Russia’s full-scale military invasion of Ukraine in February 2022 undermined internet freedom in the country. The aggressive disinformation campaigns originating primarily from Russia or linked to Russian actors sought to mislead users regarding the war, intentions of Ukraine and the Western actors. Therefore, the Ukrainian government imposed martial law, restricting freedom of expression and Government websites and news outlets were frequent targets of cyberattacks, usually by Kremlin-linked actors, that began in the days leading up to the attacks and it lasted until the end of the period covered but the Ukrainian government managed to defend itself against significant cyberattacks. The Freedom House assessment of Ukraine as “partly free” reflects the limitations on certain freedoms of information which the country has had to implement because of the war.¹⁹

Country 	Total Score and Status	Obstacles to Access	Limits on Content	Violations of User Rights
Ukraine	59  Partly Free	18	21	20

Table 2: Freedom House Score for Ukraine

Case Study: The Republic of Moldova

While women and girls in the Balkans and Eastern Europe, including Moldova, are exposed to digital gender-based violence, there remains a lack of comprehensive research and statistics specific to the region.²⁰

As elsewhere, in Moldova, there is an increase in technology-facilitated violence against women.²¹ According to the Group of Experts on Violence Against Women and Domestic Violence (GREVIO), online and digital vio-

¹⁹ “Ukraine: Freedom on the Net 2022 Country Report.” Freedom House (2022). <https://freedomhouse.org/country/ukraine/freedom-net/2022>.

²⁰ “How Online Violence against Women Goes Unpunished”, *Balkan Insight* (May 11, 2022), <https://balkaninsight.com/2022/05/11/how-online-violence-against-women-goes-unpunished/>.

²¹ Country Gender Profile. (2021). Republic of Moldova, EU4 Gender Equality. Reform Helpdesk. <https://euneighbourseast.eu/news/publications/country-gender-profile-of-the-republic-of-moldova/>.

lence against women and girls is catalysed through the amplification of sexism online, further entrenching gender inequality.

Sexist language, harassment, persecution, posting of non-consensual intimate material, and blackmail are among the forms of violence against women and girls using technology.²² According to the European Council guide for assessing and processing hate speech cases, there is an increasing number of cases of hate speech and discrimination in the public space and the media in the Republic of Moldova.

The election campaign for the presidential elections of 1/15 November 2020 was marked by intolerant public speeches, and the dynamics of hate speech and incitement to discrimination increased in intensity during the pre-election and election period and decreased after the end of the election campaign.

The relevant Moldovan media legislation, and in particular the Audiovisual Media Services Code (the Code) provides the Audiovisual Council with legal leverage for monitoring and sanctioning cases of hate speech and discrimination recorded in the audiovisual media, including in election campaigns. However, for the effective application of the provisions of the Code, the Audiovisual Council needs an enhanced internal mechanism for monitoring hate speech and collecting disaggregated data.

Generally speaking, Moldova demonstrates concerted efforts to combat gender-based violence and protect survivors through various initiatives of the National Agency for the Prevention and Combating of Violence Against Women and Domestic Violence,²³ UN Women²⁴ programmes in Moldova, ratification of CEDAW,²⁵ progressively amending laws and policies to enhance women's rights and labour force participation.

²² Liliana Istrate-Burciu, Rodica Moraru-Chilimar, "Gender-based violence in the Republic of Moldova in the context of the humanitarian crisis produced by the war in Ukraine", UN High Commissioner on Refugees, n.d.

²³ Moldova's National Agency for the Prevention and Combating of Violence, <https://anpcv.gov.md/en> (in Romanian).

²⁴ "What we do: Ending violence against women", UN Women – Moldova, n. d. <https://moldova.unwomen.org/en/munca-noastra/ending-violence-against-women>.

²⁵ "Know Your Rights! Be Protected! Convention on the Elimination of All Forms of

Case Study: Ukraine

Online violence in Ukraine often intersects with political views. Women, especially those vocal about issues like the Russian war against Ukraine, face gendered threats, hate speech, and doxing.²⁶ The online violence also has a dimension of nationalist rhetoric, further complicating the issue.

The Russian war against Ukraine continues to have a significant impact on the human rights. Early in the crisis, gender-based violence, including conflict-related sexual violence, intimate partner violence, sexual exploitation/abuse, and trafficking, coupled with online harassment and violence was identified as a significant issue.²⁷

Civil society has been active, with organizations like the Femen movement raising international awareness on the issues of gender violence, both online and offline.²⁸ The Ukrainian government has begun to recognize online violence as a genuine threat, but legislation is still in nascent stages. Tech companies, influenced by global trends, in Ukraine has enacted legal measures to address online gender-based violence, reflecting a commitment to protecting individuals in the digital sphere: Council of Europe General Recommendation addresses gender-based violence against women in the digital realm. It proposes actions aligned with the pillars of the Istanbul Convention, emphasizing prevention, protection, prosecution, and coordinated policies. Ukraine's approval of the Istanbul Convention on preventing violence against women encompasses online violence.²⁹ Ukrainian legislation mandates that personal information about survivors and those reporting gender-based violence should remain confidential, safeguarding their privacy and rights.³⁰

Discrimination against Women – Easy-Read-Version of Selected Articles”, UN Women – Moldova, (2017). <https://moldova.unwomen.org/en/biblioteca-digitala/publicatii/2017/07/cedaw>.

²⁶ Human Rights Watch, “Gendered online violence in Ukraine”, (2020).

²⁷ Securing Gender Equality in Ukraine Amidst the War. <https://eca.unwomen.org/en/digital-library/publications/2023/02/securing-gender-equality-in-ukraine-amidst-the-war>.

²⁸ Femen's Official Report. (2019). Online violence faced by activists.

²⁹ Council of Europe, “Ukraine reinforces safeguards against domestic and gender-based violence”, n. d. <https://www.coe.int/en/web/execution/-/ukraine-reinforces-safeguards-against-domestic-and-gender-based-violence>.

³⁰ Council of Europe, “Ukraine reinforces safeguards...”.

Due Diligence

The due diligence principle obligates States to take reasonable action to address and eliminate violence against women, whether committed by the State or non-State actors. The Due Diligence Project, initiated/developed by the Office of the High Commissioner for Human Rights, looked at State compliance in five areas, namely prevention, protection, prosecution, punishment and provision of redress and reparation (5Ps) and developed a Due Diligence Framework on State Accountability to Eliminate Violence against Women.³¹

The United Nations defines human rights due diligence as a process by which enterprises “proactively manage potential and actual adverse human rights impacts due to actions of the companies.”³² These processes include four key components: Identifying and assessing actual or potential adverse human rights impacts, integrating findings from impact assessments to mitigate effects, tracking the effectiveness of mitigations, and communicating on how impacts are being addressed. Human rights due diligence processes can vary in scope and structure depending on risk, ranging from cursory reviews to assess risk, to more robust product or project-level human rights impact assessments, to comprehensive enterprise-level human rights impact assessments. Due diligence can be carried out rapidly or over longer time frames depending on the circumstances, though internal expertise or with the assistance of external experts depending on the subject matter.

The purpose of this framework is to establish normative criteria to assess the human rights-related and gender-based violence-related risks pertaining to harms directly caused by the tech platforms and social media, contributes to, or is indirectly linked to and influenced by potential external events, activities, relationships, or circumstances.

³¹ OHCHR, “Eliminating online violence against women and engendering digital equality”, <https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/GenderDigital/DueDiligenceProject.pdf>.

³² “OHCHR Corporate Human Rights Due Diligence – Identifying and Leveraging Emerging Practices.” n.d. OHCHR. <https://www.ohchr.org/en/special-procedures/wg-business/corporate-human-rights-due-diligence-identifying-and-leveraging-emerging-practices>.

Social media platforms, integral to the modern digital landscape, unfortunately also serve as venues for pervasive online harassment, often transcending various online spaces and borders (UNSRP, 2019). For instance, a PEW Research survey from 2017 emphasized the heightened vulnerability of younger adults to online harassment, with a staggering 67% of individuals aged 18–29 having experienced it.³³ Even more concerning, the survey highlighted that gender-based violence distinctly impacts women, especially younger ones.

Additionally, the FRA’s survey in 2014 from 28 European countries revealed concerning data: 11% of women encountered unsolicited and inappropriate sexually explicit messages across digital platforms, while 14% faced recurring hostile messages or phone calls from the same perpetrator.³⁴

Such gender-driven infringements online not only violate individual privacy rights but are deeply connected to broader issues of violence and discrimination. Their persistence underscores an apparent inertia by State and non-State actors in addressing them, leading to an unsettling consensus that such grave infringements are somehow passively accepted.

In a broader context, these infringements denote a systematic denial of human rights, having ripple effects that perpetuate existing unequal societal structures. As technology becomes more embedded in daily lives, the resulting damages from tech-induced privacy breaches, such as cyberstalking or unwarranted surveillance, bear significant consequences for individuals and societies.

Given the expansive influence of digital platforms and the world’s increasing dependency on them, it is untenable to overlook their ramifications on fundamental human rights. This highlights an urgent need for private companies, especially those in social media, to align their operations with human rights standards. At the same time, states are obligated under the principle of

³³ Maeve Duggan, “Online Harassment 2017”, *Pew Research Center: Internet, Science & Tech* (July 11, 2017), <https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/>.

³⁴ Fundamental Rights Agency, “Violence against Women: An EU-Wide Survey Main Results” (2014), https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

due diligence to uphold the international rights framework that denounces gender-based violence and champions privacy.

Embracing and operationalizing this human rights framework is paramount. With the rapid evolution of technology comes a myriad of tools that, in the wrong hands, can be weaponized to perpetrate abuse and violate human rights. Thus, vigilant public and international oversight on the actions and/or inactions of both State and private entities is crucial to prevent violence in all its forms, including technology-facilitated violence against women.

Policy Recommendations

People who experience gender violence may suffer from different human rights violations – for example the right to life, freedom from torture and degrading treatment, freedom from discrimination and the right to safety and security. All these rights can be found in international and regional human rights documents, in particular by the United Nations and the Council of Europe.

Despite the significant progress achieved with the instruments mentioned above, recognition of the severity of the problem and existing legal measures are not sufficient. Effective mechanisms and processes for violence prevention and gender mainstreaming need to be put in place. In addition to the international human rights mechanisms, important national public policies or bodies at the national level need to include:

- National committees for gender advancement with a clear plan of action;
- Equality ombudsman;
- Effective legislation to ensure legal and substantive equality;
- Affirmative action, such as quotas for women in education and employment;
- Civil society organisations have an important role in advocacy or lobbying efforts.

Online platforms, in partnership with governments and civil society, have a responsibility to try to overcome these challenges. Platform hosts must take

concrete steps to minimize the harms caused by harassment, discrimination, and violent speech.

Platforms should adopt Human Rights Policies and Strategies in order to reaffirm their commitment to upholding the human rights of their users. Among other responsibilities, Public policies should commit to carry out human rights due diligence and proactively identify, analyze, and mitigate potential human rights harm the projects may cause, contribute to, or be linked to. A lot of the external threats can be countered by:

- **Completing a Human Rights Impact Assessment** for a proposed technical project, and consulting experienced users to better understand the human rights opportunities and risks.
- **Initiating a Child Rights Impact Assessment**, and consulting experienced users to identify and analyze human rights risks to minors in order to avoid them in the future or help the affected ones.
- **Developing a Human Rights Due Diligence Framework** to guide when and how the Platforms must carry out human rights due diligence in a cohesive and systematic way, which also takes into account our limited resources to monitor and to act.
- **Build internal capacity** if the organizations providing services to vulnerable groups to mainstream online gender based violence risk mitigation in line with good practice standards set out in the gender based violence Guidelines, including capacity to identify and address risks that emerge in programs and services.
- **Establish partnerships with organizations** serving particular groups of women in order to improve their access to services, for example, by partnering to deliver outreach/mobile services, establish referral protocols, and support coordinated actions for survivors.
- **Strengthening the Accountability for social media platforms:** In view of the capacity of internet companies to facilitate and amplify online and technology-facilitated violence against women, as well their vital role in reducing and mitigating harms, steps are being taken to introduce greater regulation of internet platforms, including social

media companies.³⁵ The UN Special Rapporteur has stressed in many national reports the importance of examining regulation of the private sector regarding online and technology-facilitated violence against women.

- **Designing Education** and awareness raising campaign at the national, regional and international levels.
- **Gathering Accurate data collection** to evaluate the manifestation of online violence against women and girls, in order to introduce effective law and policy reforms.

³⁵ Office of the High Commissioner for Human Rights, *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform*, (Brussels: EU OHCHR, November 2022), https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf.