

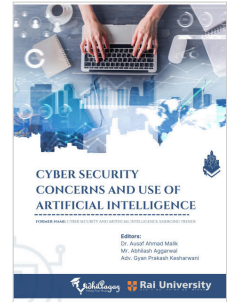
CHAPTER 33

Digital Injustice: Human Rights and the Growing Threat of Online Gender-Based Violence

Pakhi Tandon

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 271–279

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Pakhi Tandon, *Digital Injustice: Human Rights and the Growing Threat of Online Gender-Based Violence*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 271 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Pakhi Tandon, 'Digital Injustice: Human Rights and the Growing Threat of Online Gender-Based Violence' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 271.

CHICAGO (17TH ED.)

Tandon, Pakhi. "Digital Injustice: Human Rights and the Growing Threat of Online Gender-Based Violence." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 271–279. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-33/>.

APA (7TH ED.)

Tandon, P. (2024). Digital injustice: Human rights and the growing threat of online gender-based violence. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 271–279). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-33/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-33/>

RIGHTS

Free to read online. © VidhiAagaz 2024. All rights reserved: no part of this publication may be copied, reproduced, adapted or transmitted in any form or by any means without the prior written permission of the publisher.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

DIGITAL INJUSTICE: HUMAN RIGHTS AND THE GROWING THREAT OF ONLINE GENDER-BASED VIOLENCE

Pakhi Tandon⁴⁹

ABSTRACT

Online gender-based violence (OGBV) is a growing issue in today's digital world, involving cyberstalking, doxxing, non-consensual sharing of intimate images, online harassment, and hate campaigns. Women, LGBTQ+ individuals, and marginalised communities are disproportionately affected, facing violations of their rights to privacy, expression, and security. These abuses reinforce gender inequality and silence already vulnerable voices. Despite its severe consequences—such as trauma and isolation—legal frameworks lag behind. International protections like the Universal Declaration of Human Rights and CEDAW do not adequately address digital violence, and national laws on cybercrime are often fragmented and poorly enforced. Online platforms, though central to modern communication, are often not held accountable for the abuse of their services. This paper examines the nature of OGBV, its human rights implications, and the shortcomings of current laws and regulations. It also looks at the role of digital platforms in either fostering or mitigating abuse and offers recommendations for legal reforms, greater platform accountability, and digital literacy initiatives. Addressing OGBV requires coordinated efforts from governments, platforms, and civil society to protect vulnerable groups.

Keywords: Online Gender-Based Violence (OGBV), Human Rights, Digital Safety, Legal Frameworks, Platform Accountability

INTRODUCTION

The digital age has been a transitional period for social life. Its greatest opportunity for information exchange and communication is also its darkest area in making gender-based violence likely, targeting women, gender minorities, and sexual minorities. Online gender-based violence (OGBV) refers to harmful or discriminatory behaviours that are menacing or threatening within a digital context, directed at one or more individuals based on their perceived or actual gender or sexual identity.

OGBV cannot be described as a standalone issue but forms part of a much broader spectrum of GBV, deeply ingrained in patriarchal systems and societal inequalities. In the context of human rights, OGBV violates fundamental freedoms—the right to be free from violence, the right to privacy, and the right to freedom of expression. The victims of OGBV face insurmountable barriers to seek justice, as legal frameworks lag behind technological advancement, and the online platform is not taking enough responsibility for violence that gets perpetrated on it.

This paper discusses the dynamics of OGBV; its impact on human rights for women and other gender-disadvantaged groups, and whether international and national laws are effective in dealing with this issue. It also examines how online platforms promote OGBV and what policies can be employed to counter the rising menace of OGBV to human rights on the digital platform.

DEFINE ONLINE GENDER-BASED VIOLENCE (OGBV)

The characteristics and features of OGBV

⁴⁹ Student at Christ (Deemed to be University) Pune, Lavasa, India.

Online gender-based violence (OGBV) refers to various forms of abusive conduct conducted through digital channels, including social media, websites, and messaging applications. Although the internet serves as an essential resource for information dissemination and personal expression, it has simultaneously emerged as a medium for gendered violence, taking advantage of the anonymity, rapidity, and lack of geographical boundaries inherent in online communications.

OGBV can be divided into several categories:

1. Cyberstalking refers to the continuous and unwelcome digital observation or communication, typically resulting in anxiety or psychological discomfort. This form of harassment often disproportionately affects women, as offenders closely observe their online actions and employ digital means to exert control or influence over their conduct.
2. Doxxing: The process where personal information like people's home addresses, phone numbers, or personal identification details are made public without their consent. Doxxing is a technique used to intimidate and harass their victims, which may later lead to violent acts in real life.
3. Non-consensual sharing of intimate images (Revenge Pornography): The non-consensual sharing of intimate or sexually explicit images of a person is the most common type of OGBV. It usually serves the purpose of embarrassing, extorting, or dominating the victim.
4. Online Hate Speech and Cyberbullying: Women and other gender minorities are often targeted through hate speech, threats, derogatory comments, and cyber-sexual harassment online and in almost every other virtual context. Online harassment is used to intimidate, humiliate, or terrorise the victim, making these spaces unsafe.
5. Trolling and Flaming: Trolling is characterised by the intentional provocation or distress of individuals on the internet, frequently through insulting or offensive remarks. Flaming denotes aggressive online exchanges marked by hostile language, often aimed at individuals based on their gender or sexual orientation.
6. Identity Theft and Impersonation: Certain offenders construct fraudulent profiles utilising a victim's name or likeness with the intent to mislead others, disseminate false information, or tarnish the victim's reputation. Such actions may result in harassment, financial deception, and social alienation.

OGBV represents a manifestation of entrenched power disparities within society, wherein online platforms perpetuate and intensify existing gender hierarchies. This phenomenon disproportionately impacts women, while gender minorities and LGBTQ+ individuals are similarly subjected to increased risks. Additionally, intersectional dimensions including race, ethnicity, and socioeconomic status further aggravate the experiences associated with OGBV, as women of colour and individuals from marginalised communities frequently suffer from multifaceted types of online harassment.

PREVALENCE AND EFFECT OF OGBV

Underreporting, variation in definition, and a lack of uniformity in data collection between jurisdictions make it quite challenging to quantify the scale of OGBV. However, many more studies established that the problem was ubiquitous. For instance, a survey done by Amnesty International in 2018 reported that 23% of women from eight different countries reported experiencing online abuse or harassment; for those, the psychological and emotional impact was understandably prominent, with many reporting increased anxiety, depression, and feelings of insecurity.

The incidence of cyberbullying among individuals who identify as LGBTQ+ is significantly increased. Studies have shown that LGBTQ+ individuals suffer much greater rates of intimidation, threats, and hate speech, often driven by homophobic, transphobic, and misogynistic attitudes. The attributes of anonymity and the vast international extent of the internet provide perpetrators with a sense of immunity, leading to growing numbers and more extreme forms of violence.

The consequences of OGBV go beyond the digital sphere: long-term psychological trauma, social isolation, and professional setbacks for victims, and the complete withdrawal of women and marginalised people from online spheres as a whole, leading to a chilling effect on free expression and engagement in public discourses. Self-censorship limits the diversification of voices and perspectives in digital conversations, further cementing existing power imbalances and gender inequalities.

OGBV AS A VIOLATION OF HUMAN RIGHTS

Online gender-based violence goes beyond being a violation of personal rights; it violates crucial human rights. The internet is an essential space through which many rights such as freedom of expression, access to information, and political involvement are exercised. Online gender-based violence undermines all these rights by creating a hostile and dangerous environment for women and other marginalised groups. Underlying human rights affected by online gender-based violence include:

- **Right to Privacy:** OGBV often relates to invasions of personal privacy, including issues such as doxxing or the non-consensual sharing of intimate images. Such acts subject the victims to harassment and threats up to actual physical harm, violating the fundamental right to privacy and security.
- **Freedom of speech:** Women and gender minorities face web harassment while they try to communicate themselves or in public speech. The fear of abuse or backlash deters many to pre-censor themselves or refrain altogether from engaging online, thereby limiting their right to free expression.
- **Right to Security and Freedom from Violence:** OGBV is a form of gender-based violence that violates the right to live free from violence, discrimination, and harm. The psychological, emotional, and physical consequences of OGBV are severe, and, in extreme cases, threats transmitted through online platforms become real violence.
- **Right to Dignity and Equality:** OGBV reinforces gender stereotypes, thus perpetuating gender inequality. The abuse mainly affects women and members of the LGBTQ+ community, whose dignity is offended and further contributed to a culture of discrimination and violence.

FRAMEWORK FOR HUMAN RIGHTS CONCERNING OGBV

International Legal Systems

International human rights law sets the framework for the approach to OGBV, although it does not focus specifically on the digital dimensions of gender-based violence. The following is some key international instrument relevant to OGBV:

1. Universal Declaration of Human Rights (UDHR): The UDHR is one adopted in 1948 that addresses the basic rights and freedoms to which all individuals are entitled. Article 3 provides for the right to life, liberty, and security, while Article 12 undertakes to guarantee respect for privacy. Although the UDHR predates the digital age, the principles it contains are relevant to OGBV in that online violence and harassment infringe the right to privacy, security, and dignity.

2. The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which was ratified in 1979, represents a significant international agreement aimed at eradicating discrimination directed at women. Article 1 delineates discrimination as any form of distinction or limitation based on gender that hinders the fulfilment of human rights. CEDAW mandates that nations implement actions to eradicate violence against women, a mandate that includes addressing such violence within digital environments where online gender-based violence (OGBV) transpires.

3. International Covenant on Civil and Political Rights (ICCPR): The ICCPR, established in 1966, ensures fundamental civil and political liberties, encompassing the right to privacy (Article 17), freedom of expression (Article 19), and safeguards against discrimination (Article 26). The occurrence of OGBV infringes upon these rights, especially by restricting the freedom of expression of victims and exposing them to violations of their privacy.

4. Istanbul Convention: The Istanbul Convention is the full name of the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence. It is one of the most general agreements dedicated to gender-based violence. Primarily, it tends to underscore

5. Off-line violence: It calls for criminalization of some forms of online misconducts by states, such as stalking and sexual harassment.

Although such instruments provide a very robust framework on which to frame attacks against GBV, they have remained deficient specifically with regard to modern violence in their digital nature. With growing prevalence more and more in conjunction with OGBV, there must be recognition and a concrete way of finding a solution to challenges that online abuse carries within international treaties and conventions.

National Legal Frameworks

The efforts at the national level have been quite different in different jurisdictions, with some countries making quite remarkable progress and others not doing so well at all. Most countries have amended harassment, defamation, and stalking laws to include digital crimes, but these amendments are mostly piecemeal and not adequate enough for the general OGBV situation.

1. The United States. In the United States, there is no federal legislation that specifically focuses on OGBV. However, there are numerous state laws on the books which specifically address aspects of the issue, such as the more specific cyberstalking and revenge porn statutes. Though VAWA and CDA do provide some protections, a lack of a unified federal approach regarding OGBV represents an important gap.
2. EU: The EU has made strides in combating Online Gender-Based Violence (OGBV) through efforts like the General Data Protection Regulation (GDPR), which specifically aims to protect personal data, and the Digital Services Act, which aims to hold online platforms accountable for such detrimental content. In the meantime, enforcement and heterogeneity among its member states remain a challenge.
3. India: The country has enacted legislation, the Information Technology (IT) Act, that holds legal consequences for cyber stalking, doxxing, and revenge porn. However, application varies, and stigma in society leads most of the victims not to come forward with incidences of OGBV.
4. Philippines: The Philippines enacted the Cybercrime Prevention Act in 2012. It encompasses some forms of cybercrime like cyberstalking, identity theft, and hacking. This country has been praised for its foresight on digital crimes, but some critics said a few provisions are particularly dangerous against free speech because they pertain to libel.

In many countries, the enactment of laws responding to OGBV is affected by the activities such as underreporting, ignorance of law enforcement, and judicial incompetence in terms of perceiving the seriousness of online violence.

OBSTACLES IN TACKLING OGBV

Accountability of Platforms and the Function of Technological Corporations

Perhaps the greatest challenge to tackle OGBV is the role of online platforms and tech firms. Social media sites, messaging apps, and websites are the means whereby most OGBV takes place, and yet companies have been very slow to take effective action to prevent abuse.

1. Inconsistent Enforcement of Community Guidelines: Many online platforms have community guidelines that prohibit harassment, hate speech, and other forms of abuse. However, enforcement is often inconsistent, and harmful content frequently remains online despite being reported by users. This inconsistency undermines trust in the platforms' ability to protect users from OGBV.
2. Limitations of Content Moderation: Automated systems for content moderation, which are employed by platforms such as Facebook, Twitter, and YouTube, frequently struggle to effectively identify subtle manifestations of abuse, especially in cases involving gender-specific slurs, coded language, or non-verbal content, including images and videos. Human moderators are frequently inundated by the sheer amount of content, resulting in delays or shortcomings in responding to reports of abuse.

3. **Profit Motives and User Engagement:** Most technology company business models are driven to a great extent by user engagement, which promotes the acceleration of abhorrent or harmful content. Twitter and Instagram make money through increased user engagement even if it is fueled by abuse or harassment.
4. **Lack of Transparency:** Most websites are not transparent about how they address reports on OGBV. Thus, it has become very challenging for users to have an overview of the processes instituted towards the handling and abuse case. Transparency reports, when available, are usually not clear enough on the actions that were undertaken in ensuring non-accessible harmful content or having offenders punished.

Legal and Jurisdictional Obstacles

The internet's global nature poses significant legal challenges in handling the issue of OGBV. Main barriers include:

1. **Cross-border Jurisdiction:** The very reason perpetrators and victims of OGBV often find themselves on different sides of the border makes it complicated to engage in prosecution. National laws may not extend beyond borders, and international legal cooperation is often slow or nonexistent in cases of OGBV.
2. **Gaps in Law.** Most countries lack laws targeted at OGBV, especially in new ways of abuse created through deep fake pornography or coordinated harassment campaigns. Where there are laws, they are outdated or too narrow and don't include a comprehensive list of new forms of online abuse.
3. **Underreporting and Social Stigma:** Several factors give rise to severe underreporting of OGBV, such as fear of retaliation against them or their families, the lack of trust in law enforcement, and social stigma towards victims of online abuse. Victims often believe reporting OGBV would not lead to any meaningful action or would lead to further harassment and shaming as a consequence of reporting.
4. **Limitations in the Law Enforcement:** Even after reporting OGBV, the law enforcement agencies are not adequately prepared to tackle digital crimes. Most officers neither have training nor technical skills to investigate online abuse which leads to indifferent attitudes or failure to act on complaints.

CASE STUDIES: RESPONSE TO OGBV

South Africa: Feminist digital activism

South Africa has emerged as one of the centres of feminist digital activism, partly because gender-based violence is dramatically increasing in both the physical and online worlds. The AmINext movement, initiated during 2019, followed a list of women who were killed and brought attention to an even deeper issue: gender violence in South Africa. Advocates used social media, particularly Twitter and Instagram, to highlight how deeply seated violence against women was within both the online and offline environments.

Consequently, the South African government enacted laws in a response measure towards the movement, among which were reforming domestic violence laws, amendments relating to sexual offences, and cybercrimes. These are for the welfare of OGBV victims where provisions are catered for, dealing with OGBV, especially cyberstalking and online harassment.

India: Legislation Reforms under Modern Context

In India, the increasing incidence of OGBV has led to legal reforms aimed at increasing protections for victims. The Information Technology (IT) Act 2000 was amended in 2008 with provisions that added cyberstalking, identity theft, and the unauthorised release of intimate images to the list of crimes. Furthermore, amendments made to the Indian Penal Code in 2013, following the notorious Nirbhaya gang rape, provided more severe punishment for crimes associated with sexual assault, which include online abuse. These reforms notwithstanding, enforcement remains a challenge in India. Many victims of OGBV say that law enforcement officers dismiss their online abuse, or they do not possess technical competence to investigate digital crimes more effectively. A significant number of women refrain from reporting incidents of OGBV due to social stigma and victim-blaming.

The European Union: Common Efforts to Combat OGBV

The European Union has taken a harmonised approach towards fighting OGBV, especially through policies such as the GDPR and the Digital Services Act. The GDPR, which has been in effect since 2018, brings high-level protections for private data, forcing companies responsible whenever user privacy is violated. Not particularly addressing OGBV, the GDPR is essential in checking other forms of abuse such as doxxing or identity theft.

The European Union has been frontrunner in addressing the online platforms' engagement with OGBV. The Digital Services Act 2022 is primarily aimed at building a safer online sphere by regulating the content moderation practices of technology companies. The DSA requires the content moderation practices of platforms to be more transparent regarding their algorithmic functioning and processes for removing content, in addition to introducing penalties for non-compliance with user safety regulations.

RECOMMENDATIONS FOR COMBATING OGBV

The fight against OGBV and protection of human rights of women and marginalised gender groups is absolutely necessary to be done on a multi-faceted level: legal reform, responsibility ensured from the networks, and empowerment of victims together with education in the use of digital technologies.

Improving Legal Institutions

1. International Cooperation Due to the global character of the Internet, international cooperation is necessary to address the phenomenon of OGBV. A multilateral treaty on OGBV may thus offer a framework to harmonise domestic laws across borders, establish cross-border enforcement, and hold perpetrators accountable.
2. National Legislation: Specific laws targeting OGBV should be enacted or updated to include emerging forms of abuse, like deep fake pornography, revenge pornography, and coordinated

harassment campaigns. Law enforcement and judicial authorities should receive proper guidance through a well-defined legal framework to address OGBV effectively.

3. Capacity building for law enforcement: Equip law enforcement agencies with the necessary capacity and skills to address the cases of OGBV. Such necessary capacities include training in digital forensics as well as in a victim-centred approach to handling online abuse cases.

Holding Platforms Accountable

1. Transparency and Accountability: The enabling role of OGBV by online platforms should be made accountable. Governments should introduce compulsion for the online platforms to come with transparency reports that will detail how they respond to complaints against abuse, the steps taken, and resultant outcomes.
2. Enhanced Content Moderation There should be sufficient content moderation on the systems, especially when using AI in detecting dangerous content and more human moderators to sort out abuse in nuanced cases. The reporting mechanisms of these platforms should also be enhanced to make it easy for victims of OGBV to file complaints and receive responses.
3. Data Protection: Governments should strengthen data protection laws in position to ensure that online platforms can't misuse user data, nor endanger the person to the risk of OGBV. This should include holding companies liable for breaches of privacy issues, such as doxxing and the unauthorised publishing of private images.

Empowering Victims and Digital Literacy

1. Support Systems: Availability of support structures to OGBV victims entails legal, psychological, and reporting mechanisms for individual security. These support systems can come from governments and civil society organisations collaborating together.
2. Digital Literacy: Raising awareness about online safety and digital rights is essential in preventing OGBV. Schools, universities, and NGOs should incorporate digital literacy programs that educate users on how to protect themselves online.
3. Support Reporting Governments and service providers must ensure that a safe environment exists for reporting OGBV. This includes, among other things, ensuring complainants are not retaliated upon at the reporting stages and ensuring their concerns are taken seriously.

CONCLUSION

It therefore poses a significant threat to human rights in the digital era by increasing online gender-based violence. As much as new forms of interaction and expression are facilitated through technological innovations, it has equally enabled exploitation. OGBV also threatens vital human rights, especially those of privacy, security, and freedom of speech. There is a need for legal frameworks at both the national and international levels to evolve with these new challenges. In addition, online services must also be held accountable for their role in facilitating abuse. Combating OGBV requires a collaborative, worldwide approach combining legal reform, platforms' responsibility, and digital literacy to protect women's and all marginalised gender groups' human rights.
