Journal of Law & Social Studies (JLSS)
Volume 7, Issue 1, pp 26-42
www.advancelrf.org

Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions

Tooba Nazakat
(Corresponding Author)
LLB Student, Faculty of Shariah and Law, International Islamic University, Islamabad (IIUI)
Email: toobanazakat02@gmail.com

Faiza Eiman Malik
LLB Student, Faculty of Shariah and Law, International Islamic University, Islamabad (IIUI)

Abstract
This paper scrabble around multipart issues of Technology-Facilitated Gender-Based violence (TFGBV) by scrutinizing the overlap between Artificial Intelligence (AI) and legal strategies sighted at diminishing widespread obstacles. Examine the legal structure focused on the effectuality of operating laws engaging in the Technology facilitated Gender Based violence, suggesting improvements and new policies to make invulnerable shield for victims. This paper center on the technological advancements, on the dual role of Artificial Intelligence both as the contrivance exploit to encourage TFGBV and also as a strong collaborator in hinder it, that could aid law enforcement in dispatching justice. Challenges look on to law enforcement and judiciary in taking up TFGBV are underlined, initiating methods to impel response and appropriate justice, stressing the necessity for specialized training and resources. Acknowledging the divergent encounter of victims, paper emphasizes the essentials for justice system to embrace the approaches that examine interesting identities such as sexuality, race, disability, which affect victim experiences and desire reshape legal responses. By comparative research of international approaches to TFGBV discloses constructive policies for counters against online harassment. This paper focused on the balancing sufferer privacy, observation, and unties speech instructions for managing digital verifications. The paper inspects the role of international agreements in acknowledging TFGBV, underling how they can strengthen global endeavors. This paper focused on accommodate the Artificial intelligence and legal framework to flourish and extensive paths to TFGBV, connecting technological innovations with sturdy legal manners strengthen victims protection and grantee offender answerability.

Keywords: Gender-Based Violence, Artificial Intelligence, Cyberbullying, Legal Frameworks

1. Introduction

Technology Facilitated Gender-Based Violence (TFGBV) is an escalating global issue, which is affecting the vulnerable groups of population including women, young girls and children. Particularly professional women for example journalists, politicians etc. have been the major target of TFGBV. Men have also been a target of TFGBV but the ratio is quite low as compared to women. TFGV could be due to multiple factors for instance due to ethnicity, gender expression, refugee status, sex characteristics, religion, ability, gender identity, etc. (Technology-Facilitated Gender-Based Violence Program (TFGBV) Globally, 2023) It has profound social, economic and health consequences not only affecting specific groups but society at large. It has limited women's productivity, as a victim of TFGBV, it does not only cause material harm, but it also has significant effects on their mental health making it harder for the women to participate in their everyday life tasks. Women also have to face financial consequences because after being subjected to Non-consensual Intimate Image Distribution (NCIID) they are expelled or fired from their jobs or sometimes they choose to leave their jobs because it influences their reputation as well. As social beings, humans rely on interaction with others

to navigate societal structures. However, for individuals who have been victimized and whose reputations have been affected, reintegrating into social networks can become increasingly difficult. Society often stigmatizes these individuals, creating barriers to meaningful social engagement and further isolating them, which hinders their ability to rebuild and participate fully in community life. Women are also being restricted in public participation for instance suppressing women voices that's why women's representation in their society is proportionally less than men. Consequently, this disparity is not only an alarming threat to private life but public life as well.

The rate of TFGBV offenses increased rapidly during the COVID-19 pandemic because people were more exposed to online world than physical one. As all activities were being carried out by technology with the aim of minimize the expansion of virus in world, there were enough possibilities of increased rate of TFGBV.

For the past few years, the advancement of Artificial Intelligence (AI) has created new areas providing significant ways to combat against TFGBV. AI technology has been used in identifying and preventing the TFGBV. It has provided various ways to tackle with this offence including content moderation systems, algorithm detection of harmful content etc. These tools are being used to flag abusive content in real-time, remove harmful posts and identifying online abuse before it becomes more severe. However, certain limitations to the AI can be observed. Bias in algorithms can silence the marginalized voices. Moreover, privacy concerns and inefficiency of AI to detect nuanced text complicates it effectiveness.

Simultaneously, the existing legal frameworks have been evolving with the advancement of technology. There are various International and National Legal frameworks addressing offences related to TFGBV. However, a comprehensive approach to deal with TFGBV by the use of the advanced technology in the form of AI combined with legal strategies can result in outstanding solutions for eradicating TFGBV.

2. What is TFGBV?

Technology Facilitated Gender-Based Violence can be studied by dividing it into two parts: Technology Facilitated and Gender-Based Violence (GBV). To understand how GBV is being facilitated through Technology first we have to understand the concept of Gender-Based Violence.

Gender-Based Violence is an abuse carried out against an individual because of his gender or use of force that influence individuals of distinct gender disproportionality. GBV contributed to psychological, physical corporeal and monetary damages or sexual harm as well. (What is gender-based violence?) The gender based violence, united nation has described it in “Declaration on the Elimination of Violence against Women", 1993.

In Article 1 it is outlined in these words:

"That results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."

TFGBV is carried out through different digital platforms and tools for instance it includes social media (Facebook, YouTube, Snapchat, Instagram, X and so many others), messaging apps, (whatsapp, telegram etc.), and many other online spaces including zoom, Microsoft team etc. This form of violence involved the wrong use of both existing and emerging technologies, incorporating hardware and software, and frequently modifying as technology develops. International Centre for Research on Women (ICRW) defines TFGBV as:

"TFGBV is action by a person or a group that bring suffering to others grounded on their gender or sexual identity or through implementing destructive gender practices. This action is performed

making use of the Internet and/or mobile technology and comprises bullying, stalking, defamation, sexual harassment, exploitation and hate speech." (L. Hinson, 2018)

There is a chain between TFGBV and GBV, often the violence created in cyberspace may lend a hand to offline GBV as well. (Ruth Lewis, November 2017) A study was conducted in Malawi that 53.7% women had experienced physical abuse followed by the online violence making their situation worse and about 34.3% of these women had to face harmful consequences as an impact of that online violence. (Malanga, 2020)

TFGBV can be committed in various form, few of them are discussed below:

CYBERSTALKING	Using digital platforms or social media platforms for instance Instagram, Facebook, email, or messaging apps to monitor someone frequently over the time, to harass or threat. Cyberstalking also involve unwanted messages, tracking someone online, or spread misinformation.
DEEPFAKES	Deepfakes are AI generated videos, images or audios to make someone appear to do or say something which he actually didn't do so or make a fake controversial statement. Deepfakes are growingly misused for the purpose of creating sexual images without consent such as photoshoping faces of women on porn images.
IMAGE BASED ABUSE	When a person creates, shares or threats to share intimate images without consent or harass or abuse by using it, refers to Image Based Abuse.
SEXTORTION	When a person has a sexual image of an individual and used it as a threat or coercion against that person compelling him to do something, which he doesn't want to do. This form initiates sextortion.
DOXING	Non-consensual sharing of private, personal and sensitive information including home address, work place, and contact numbers and so on, on online platform refers to doxing.

3. Legal Frameworks: Adapting the Digital Era

For the past few years there has been an explicitly robust advancement in the field of technology which has ultimately given rise to the need of legislation in this field as well. It is well understood that where the technology has opened doors to the opportunities thereby it has created path to the new offences and Gender Based Violence rank among these. The world observing the rising rate of the Online Gender Based Violence (OGBV) has legislated the laws internationally and nationally.

For decades various countries have enacted laws dealing with the TFGBV. Greater Cooperation is made towards control of TFGBV by Governments, NGOs, and Law enforcement. The general concept that should be followed is whether the offence occurs in physical space or cyberspace, relevant law should be applied regardless of such fact. For example; In Pakistan, the Prevention of Electronic Crimes Act, 2016 was passed addressing the cybercrimes. Several sections of PECA prohibit harassment, child pornography, cyberstalking and unauthorized access to personal data. PECA has covered substantial aspects of TFBGV but it is subject to certain limitations as well.

Some states have formulated laws targeting some explicit categories of TFGBV, including Indonesia's Undang-Undang Tindak Pidana Kekerasan Seksual (UU TPKS), in English, the Law on Electronic Based Sexual Violence. This law restricts the recording of sexual content in addition to its broadcasting in the absence of consent and also prohibiting the stalking of people for any sexual purposes and exploitation. (Sarah, 2022) Jordan's Law on Electronic Crimes Number 17/2023 has

introduced an article in it providing protection against pornography cybercrime. (Evon Abu-taieh, 2019) In South Africa, the Harassment Act (2011) helps harassment victims to take action against the harassment perpetrators including TFGBV. (Protection from Harassment Act, 2011).

Progress is being made at international level as well. Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) also known as International Bill of Rights for Women was adopted by UN assembly for the purpose of ensuring that women are provided with same rights as men without any discrimination. International Centre for Research on Women (ICRW) has been advocating for the rights of women and proposing various policies for their protection against TFGBV. (Landscape Analysis of Technology-Facilitated Gende-Based Violence: Findings frim Asia., 2022) UN women have stated that current laws have failed to keep up with the progress made in technology. This has given rise to increased public demand for the establishment of policies and laws for the purpose of accountability.

Digital Services Act (DSA) is new legislation introduced in Europe in 2022 which has set out the provisions for the liability for illegal content, Obligations for very large platforms (VLOPs), protection of fundamental rights and transparency and accountability.

Even there are several laws existing for the purpose of protection against TFGBV but the scope of these laws is very limited as most of these are only targeting specific forms of TFGBV. Moreover, the technology at the time when these laws were enacted was not developed at the same level as it has advanced in the past few years, which is enough to prove that these laws are outdated and in extreme need to be revised and updated in accordance with the current advancements made in the field of technology.

4. The role of AI in Diminishing TFGBV

With the evolution of man, technology has also. A great debate has taken place that the technology especially AI is effecting our society. The rapid advancement in AI make it easier for any one, in past only experts could use it but now it is easy to use even by a lay man just on one click which makes it more dangerous or harmful. AI is a broad field that includes technologies like machine learning and deep fakes, the latter of which is often used to target women through non-consensual, pornographic videos. AI commonly has known through its brand names e.g. Midjourney, Chat GPT, Gemini, Chabot, Dall-E and so many others. Generative AI can create faked pictures, text, audio and even videos as well. These all lend a hand to attackers for carrying out online Gender Based Violence against their target.

Generating deep fake through AI is most familiar tool for the violence against politicians and journalists. Fake political ads become common in this age through AI. As we already observed an incident of Fake AI generated Political ad in America in 2023. (Kelly, 2023) A research by UNESCO acknowledged that 29% of women journalists faced online abuse or attack during the coverage of election between 2019 and 2022 in America. (UNESCO) A recent report of UNESCO “the chilling” observed that women journalists in distinguish and notable position be disposed to entice more lethal abuse. (UNESCO, 2019) Disinformation has been used in various countries by state as well as non-state actors to spark aggression. For instance, in Myanmar, disinformation spread on Facebook and amplified by the social media site’s AI- powered algorithms helped incite mob violence toward the Rohingya minority, featuring widespread rape and sexual assault carried out as a part of campaign of ethnic cleansing.

Women are most likely to target through these generated AI Age. Mostly women suffer from the online gender based violence because they are not familiar from the advanced technology and also have less exposure in comparison to man. A global study held, results of this study show that almost 58% woman and young girls globally has faced online abuse through the social media platforms. And most disturbing fact, that most girl experienced online violence between the age of 14 to 16 years. (UN-Women, Accelerating efforts to tackle online and technology facilitated violence against women

and girls (VAWG), 2022) A study held in Pakistan as well in which it was estimated that almost 26% women falling between the ages of 18 to 24 years have faced online exploitation, and only 7% of man with same age do so. (AI and Gender-Based Violence, 2024)

Faked image through generative AI is common in these days as in May 2023 a video circulated on social media platform Twitter in which, expulsion of Pentagon was seen that led to disinformation among the people and even it was through a verified account. (Morris, AI-generated Pentagon explosion image was shared by verified Twitter accounts, 2023) In these days almost everyone has encounter the videos or pictures of public figures, stretch from comic to detrimental. Alarming the 98% deepfake videos are pornographic in nature; 99pc target women or girls. (Dawn)

According to Pauwels (2022), researches in Israel recently produced a new method for making deepfakes in real time which require no comprehensive facial data instruction, providing "an influential software suite to generate natural-looking video forgeries at scale and with insignificant expertise"

4.1 Combating against TFGBV

AI tools, such as machine learning, can monitor online behaviors, analyze social media messages, and detect early signs of violence, enabling quick responses. Additionally, AI can gather and process data to better understand the causes of violence and identify those responsible for it. For example, a tool called "SOLIS" from Dexis has been used to analyze social media discussions about migration, showcasing how AI can reveal public sentiments and thoughts, which could potentially help identify threats before they escalate.

AI Chatbots can also use to address the TFGBV. Chatbots have been used very frequently in America and other European countries as well, to deliver information to gender based violence survivors. Sara_ the UNDP gender based violence Chatbots for central America- provide legal advice and help to gender based survivors make safety plans anonymously. (UNDP, 2023)

Another usage of AI for combating against gender based violence could be to provide facilitations against the gender based violence for instance the AI tools could be used for the measuring risk against the victim and provide them instant help. An algorithm designed to identify instances of IPV successfully identified facial injuries caused by physical violence with an accuracy of 80% (Rodriguez et al., 2021).

4.2 AI Tools combating against TFGBV

The innovation of AI tools to tackle with the increasing rate of TFGBV has been playing a significant role.

i. Sara Chatbots

AI can play an important role combating against TFGBV it can detect the threat of violence and can provide assistant to victim for instance InfoSegura Regional project, collaboration between United States Agency for International Development (USAID) and the United Nations Development Program (UNDP), launched Sara Chatbot. By use of AI, Sara secretly gives victims with instant access to vital information and resources. Sara chatbots are available 24/7 at free of cost, to provide guidance to women or others at risk of violence. Furthermore, it also assist to contact to relevant institutions in Central America and the Dominican Republic. (Artificial intelligence, toward new horizons in the fight against gender-based violence).

ii. Algorithms detect hateful speech

AI system, can analyze behavior, hateful social media messages, or detect the potential threat of gender based violence, by using machine learning algorithms. Which enable the relevant authorities to take action before the violence and provide assistant or support. An example of this is eMonitor+, developed by United Nation Development Program (UNDP) introduced in Peru, which identifies automatically hate speech and gender based violence through digital means political discussions. This

technology has significant contribute to combat against TFGBV. (Artificial intelligence, toward new horizons in the fight against gender-based violence).

4.3 Legislation in the AI against GBV

Rapid use of AI raises the concerns about security and privacy. There are many laws and regulations have been shaped on AI throughout the world.

There is some important legislation that has taken in the AI regulation field:

i. EU Artificial Intelligence Act, 2024

This act was framed against the potential vulnerability to the safety, health and rights of citizen from the AI. European Union Artificial Intelligence Act was suggested in 2021 and it was finalized in 2023 and finally it was enforced on August 1, 2024, designs to encourage superintend AI development across the EU.

The Act break down AI systems by threat proportion:

- Minimal risk: AI systems like face filter which mostly have no obligations and these can acquire voluntary standards. Article 5 of this act focused on the compilation of facial recognition data base.
- Specific transparency risk: There would be some regulations on the tools that can create illusion like chat bots, so this kind of tools must have to inform the users that it's not a human being in fact a machine.
- High risk: AI system used in censures area like health care and recruitment must have strict legislation and regulations.
- Unacceptable risk: AI social scoring applications which ranked the humans on the basis of their behavior must be banned because this can lead inequality and unfair treatment. It must be prohibited to ensure the freedom and privacy of citizens.

The European Commission has also initiated negotiation on a Code of Practice for general-purpose AI models (GPAI), concentrating on transparency, copyright, and risk management. The Code is expected to be finalized by April 2025, with feedback shaping the initiatives of the AI Office, which will oversee AI Act execution. (Communication, 2024)

This act help to minimize the violence that carry through social media platforms as the Article 52 of this act bound the technologies or apps to if the deep faked videos or images have been created it must be informed that these are not original in fact AI generated.

ii. Ethics of Artificial Intelligence Use (2023)

UNESCO has given recommendations on the Ethics of Artificial Intelligence in 2019 and again recently on 16 May, 2023 which is applicable to all 194 member states of UNESCO. These recommendations underscore the defense of human rights and nobility as its principle, nurturing transparency, fairness, and human oversight in AI systems. What sets it apart is its detailed Policy Action Areas, which enable policymakers to apply these core values across various sectors, including data governance, the environment, gender equality, education, research, health, and social well-being.

iii. Regulation of Artificial Intelligence Act 2024

Pakistan also has recognized the threats from the usage of AI through which generating deepfake videos pictures, text, and audios as well is very easy. Ministry of information and technology begin to format a policy for the AI usage in 2023 For the safety of citizen and the protection of rights of mankind and their privacy as well the senator of Pakistan Muslim League Nawaz (PLM-N) has recently introduced an act named "Regulation of Artificial Intelligence Act, 2024" in senate.

A key provision of the bill is the emergence of a National Artificial Intelligence Commission, based in Islamabad, responsible for secure fair access to AI technology for everyone, notwithstanding of their demographic and financial status. (Werner, 2024)

A key aspect of the bill is its strict enforcement measures, which state that any breach of its provisions will incur substantial fines between Rs.1.5 billion and Rs.2 billion. This provision is designed to ensure that AI systems are used safely and in compliance with the law, minimizing misuse and protecting public interests.

iv. Breaking legal barriers: Accelerating justice in TFGBV

Gaps of the Pakistan's judiciary regarding comprehension of cyberspace and its adjudication on TFGBV. The OGBV cases include aspects that are oftenly linked with offline offenses leading to sexual crimes including assault and rape.

Failed Acknowledgement of interconnectedness of the digital and physical spaces and the actual consequences of TFGBV. With the passage of time number of female Internet users is significantly increasing within the cyberspace, so is the rate of TFGBV. But so far nothing has remained totally virtual about the TFGBV. The major reason behind it is that the online violence is streaming into offline violence. UNESCO has addressed this problem as well. In UNESCO's study at 20% of women journalists have faced offline violence linked with the online violence. (Posetti, 2021) Despite of such evidence courts have neglected the fact that that online violence can lead to offline violence or vice versa. The seriousness of online violence is ignored until there is offline violence. Moreover, if the accused is alleged to commit both the online violence leading to offline violence, the courts shift their focus to the fact that the physical violence is committed, when courts should give even importance regardless of the fact that whether the violence was online or offline.

In Shemeer A v. State of Kerala, the offender not only committed the offence of trespassing, but he threatened victim to circulate her sexually explicit images on Internet and then did her rape too.

Limitations in TFGBV recognition is only because it is considered less real than physical violence. Online violence is considered non-corporeal, as it affects mental health rather than developing physical effects. Herring says that online violence is less expected and is perceived as a non-threatening crime. (Herring, 2002) But in real world technology can aid crimes against women. Victims who have suffered from OGBV have admitted that they have suffered with physical illnesses as result of the mental illness caused by the trauma. The widespread nature of this continuum calls for the Gender sensitization of the judiciary, enabling them to comprehend this issue under subject completely and address it within the framework of existing laws.

Insufficient Recognition of gendered hate speech, particularly because existing laws don't address it as offence. TFGBV includes various forms including the gendered hate speech which has remained the most unaddressed issue as there have not been any noticeable registered cases. Generally, hate speech targets an identified individual or group (can be based on gender, caste etc). Hate speech occurs via disparagement and vilification either implicitly or explicitly by proliferation of undesirable content about the targeted person on Internet.

The Council of Europe's (CoE) Additional Protocol to the Convention on Cybercrime defines sexist hate speech as,"expressions which spread, incite, promote or justify hatred based on sex". (Van Der Wilk, 2018) In India, the 267th Law Commission

Report defines hate speech as:

"Hate speech generally is an incitement to hatred primarily against a group of persons defined in terms of race, ethnicity, gender, sexual orientation, religious belief and the like (Sections 153A, 295A6read with Section 298 IPC). Thus, hate speech is any word written or spoken, signs, visible

representations within the hearing or sight of a person with the intention to cause fear or alarm, or incitement to violence."

The problem is hate speech is still not considered a part of TFGBV as it is mostly regarded in issues relating the national security and public order. Courts have not given it recognition as a gender based violence because they do not observe it as something that affects gender.

As per international practice, EU provides protection for the hate crime and hate speech. It is because of the fact that these two are not defined. So far Greece is the only state that refers to sexist hate speech in its legislation.

There are significant spaces in information known and recognition in broader scope to fight against sexist speech focused to spread hate. An initiative by CoE's Gender Equality Strategy 2014-2017 imcludes that sexism should be handled as hate speech.

v. Lack of digital evidence, reflecting challenges in TFGBV cases.

Cases of TFGBV being dealt under criminal courts lead to the burden of proof which is higher in these cases. Thus, in order to prove the charge there must be digital evidence. The challenges that prosecution had to face include bringing in testimony, providing proper documentary evidence and so on. In case State of Karnatka v. Sudeep, the prosecution was not able to produce the expert witness to prove the creation of fake account by the accused. The court noted, "The prosecution did not provide digital forensics expert and failure of not being able to trace IP address used to send texts messages to victim etc." So, in order to prove TFGBV cases which are digital in nature system has to face unique challenges.

As technology advances, Courts are faced with challenge of defining primary and secondary digital evidence in TFGBV cases. Questions that can be posed here is that: What can be categorized as primary evidence and secondary evidence? How these two can be distinguished in the case of electronic evidence? Up until now, courts consider primary evidence if one can produce the original device i.e. Laptop, mobile phones etc. However, the hard copies and other recordings of a computer output are categorized as the secondary digital evidence. But there are many gaps needed to be covered by new draft of evidence law for the purpose of alleviating the concerns like what if the screenshots of texts are produced I court? How these screenshots will be categorized? What if a deep fake of a person is created across the borders and is made accessible after bouncing off several servers, would all of these constitute as primary evidence if shown on a computer?

vi. Courts should strive to hold platforms responsible for TFGBV.

The escalation of TFGBV is because of the Social media networks like YouTube, X, and Facebook. These platforms has not only hosted but played a role fostering the violence by the rapid proliferation of the content related to GBV. A few examples can be quoted here:

- Anita Saarkeesian had to suffer from overwhelming hate only because she created a feminist YouTube series.
- A group on facebook was reported by Thorlaug Agustsdottir that posted content about women subject to abuse and with hate comments like "women are like grass, they need to be cut regularly.

Courts have to struggle with GBV committed through social media. Inability to remove the content from social media can fall within the incompetency of the police, social media platforms and the courts. Police when reach out social media platforms, these platforms ask for Letters Rogatory. They have to resort to the remedies provided by mutual legal assistance treaties (MLATs). Conversely, Social media platforms claim that removal of content is not an easy task as search engine works in a reactive way rather than proactive. These platforms claim that law can't be imposed on what can be searched on search engine. Moreover, even if they remove the typing based content it is really difficult to track picture based content as its algorithms are more complex.

The role of courts can be of more significance than police and social media platforms. Even if the content can't be removed completely but it can be made in-accessible on the orders of court by de-referencing it from search results. Court can issue such orders for search engines like Google search, Microsoft Bing, Yahoo Search etc. Court can direct Police to obtain the information regarding the offensive content from social media platforms including information like URLs, Account ID, IP address or any other information needed for the conduct of investigation. Court should emphasize that id social media platforms are only serving as the intermediaries and there is no burden on them but they are still obliged to comply with the court orders and are responsible to provide the information asked for.

vii. Lack of Framework for crossborder crimes.

The Internet is a facility that is available now for everyone and everywhere which has made it easy for anyone to target any person wherever in the world they are because everyone is connected via Internet. This fact has enabled people to take advantage of internet for committing TFGBV. The concern rising with the advancement of technology is how courts are supposed to deal with TFGBV cases when the GBV is being committed in any other country where they do not have any jurisdiction?

As the area of TFGBV Legislation is not well developed yet, so the courts often face difficulty in cases where GBV is being committed outside of the jurisdiction of courts. The difficulty arises when there are no as such prevalent laws dealing with TFGBV being committed cross borders. Moreover, there is conflict of laws. As what constitutes a crime in one state may not be a crime in other one and as TFGBV is a crime which includes many forms and all these forms have varying definitions across the world for example in Australia The Sex Discrimination Act 1984 states sexual harassment as "... unwanted conduct of a sexual nature, in circumstances in which a reasonable person, having regard to all the circumstances, would have anticipated that the person harassed would be offended, humiliated or intimidated."

In France, Article 222-33 of the French Criminal Code explains sexual harassment as, "The fact of harassing anyone using orders, threats or constraint, in order to obtain favors of a sexual nature, by a person abusing the authority that functions confer on him..." This means that someone have dominant position can only harass the other person.

Also there are extradition issues, as the local courts can't prosecute a citizen of another country. There is a need of Extradition treaties between the states which can be affected in cases where TFGBV is not prioritized in that very state. There is a possibility that a state might deny to prosecute their citizen even if the identity is known.

Different countries have varying standards for the purpose of online platforms to prevent harmful content. For example European Union's General Data Protection Regulation (GDPR) has imposed strict liability on Tech companies while America has provided much more freedom.

viii. Absence of expert judges, prosecutors and lawyers.

TFGBV might involve the technology of which judges, prosecutors and lawyers are not aware of or do not have sufficient knowledge about it. They might have to face the following obstacles while dealing with TFGBV cases:

In cybercrime cases, there is a high possibility of data being erased from the internet by the use of advanced technology for example: anonymizing networks (dark web), encryption and so on. So, Lawyers and judges need to understand how to collect, interpret and authenticate the digital evidence. Unfamiliar with the dynamic of the internet might affect the victim more. As the legal professionals who can't fully comprehend the nature and way of commission of the TFGBV can affect such cases in a very wide aspect as TFGBV can lead to severe reputational and psychological harm.

Providing Judges and lawyers if are provided with the technical training then it might create a positive impact on the TFGBV cases. Moreover, it technical studies and basic understanding of technology can be added as the part of courses of upcoming judges and lawyers.

5. Intersecting identities and their effects on TFGBV

The concept of intersecting identity can be complex, but simply put, it refers to how individuals experience advantages or disadvantages based on the combination of two or more aspects of their identity. For example, a person might be identified as both a woman and someone with a disability. Due to these intersecting identities, she may face more violence or discrimination compared to a woman without a disability. It is also known as "multiple discrimination" that refers to the discrimination that a women experienced due to multiple factor which might be based on ethnicity, race, sexuality, disability, marital status, geographical location, immigration status and so on.

There can be so many factors that relate to one another and create the violence against target for as given below:

5.1 Pubescent and Female

A report submitted to the urban institute on July 2013 by Janine M. Zweig and others in which it was said the adolescent girls experienced more online sexual abuse within the context of dating violence. (Janine M. Zweig, 2013) Another report publish by Pew research center on May 31, 2018 young females are the prominent target for the TFGBV due to their rapid involvement for the use for social media platforms. In this report it was said the almost 51% of the American teens ages between 13 years to 17 use Facebook. (Monica Anderson, 2018) An annual report shared by International Watch Foundation in 2020, in which they quoted the horrific fact, in the child sexual abuse material almost 80% is the images of between the ages of 11 years to 13 years girls. (IWF Annual Report 2020 - Face the Facts, 2020) In plan international report it was said that almost 58% of young women and teenage girls have been experience electronic harassment, reports also quoted that approximately 85% of those who have been experience more than one type of technology facilitate gender based violence, for instance it include abusive and insulting language 59%, sexual harassment 37%, stalking 32%, body shaming 39% and same ratio is the threats of sexual. (Still We Dream) In a survey of World Wide Web foundation in 2020 it was noted that almost 52 % of young female and girls have faced virtual abuse and approximately 68% of this abuse has been manifested via social media. (The online crisis facing women and girls threatens global progress on gender equality, 2020)

5.2 Female and professional life or public figure

A recent study held by UNESCO working in 125 countries with 901 journalists almost in every region found that approximately 73% women target of gender based virtual violence, and almost 20% of female journalists targeted offline as a direct consequence of such virtual violence. The women who have active engagement in social media platforms are most likely to be targeted for gender based violence as a survey held in UK, the female who have been exposed to the technology facilitate gender based violence in different forms for instance trolling, hate speech, harassment and sexual abuse as well, on Facebook 60% on blogs 46% and on twitter as well, give the ideas for the prevention of TFGBV. (Ruth Lewis, Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls, 2016) This is also very common in Pakistan the girls who are frequent users of social media platform named X are more likely to become the subject of violence and abuse the mostly users on X use very abusive language which is beyond the tolerance. Even though men are also subject of this abuse and abusive language but there is a huge difference between them and the female users.

5.3 Gender and Social Class

Sustainable Social Development Organization (SSDO) collected data from Sindh which revealed that between 1 January and April 30, 2023 there was 900 reported cases of gender based violence. And this incorporates 142 cases abuse towards children and 771 against the women. Sustainable Social Development Organization also observed that many cases go unreported due to the social stigma,

which means the actual numbers of cases of TFGV are much higher than what is officially documented. (Sharp rise in violence against women and children in Sindh during 2023, 2023)

5.4 Global approaches to tackle with TFGBV

The top approaches to deal with TFGBV are the ones having comprehensive strategies including legislative provisions and its update with time, public awareness, victim support, conducting research on TFGBV and platform accountability. Several states have reformed their laws focusing on these strategies and are discussed below:

United Kingdom in 2017 declared that they plan to make UK "the well-protected premises across nations to be networked". (Making Britian the Safest place in the world to e online , 2017)

Online Safety Act (OSA), 2023 passed by United Kingdom for the purpose of regulating online speech and media to protect public from harmful content. OSA covers three main legal duties including illegal harms, obligations for VLOPs to tackle illegal content and reporting it, protection of children. The act has the following objectives:

- Enhancing user safety online.
- Preserving freedom of speech through online mode.
- Developing users' proficiency.
- Advancing society's interpretation of the harm landscape.
- Optimizing law implementation's expertise to deal with prohibited content online.

5.5 European Union

Digital Services Act passed in 2022 by European Union. "Very Large Online Platforms" (VLOPs) and Very Large Online Search Engines(VLOSEs) are regulated under this act and are bound to remove illegal content especially the ones targeting Gender based violence. These platforms are accountable for the content they host. The DSA takes significant steps to mitigate online harm by enforcing corporate obligation and accountability, establishing documenting and supervision mechanisms, and imposing sanctions for nonconformity (Digital Services Act-Consilium)

In May 2024, the European Union passed the "Directive on combating violence against women and domestic violence. It does not only criminalize offline violence (for instance female genital mutilation and marriage under duress) but also online violence including NCIID, cyber harassment and gender-based hatred.

In March, 2024 EU passed the "Artificial Intelligence Act (AI Act), inaugural inclusive legal framework designed with the mandates that AI generated images, audio, videos, or texts must be in machine-readable format so that they can be identified as artificially generated data. (Gernort Fritz, 2024).

6. Ethical aspects of combating TFGBV

For the better and effective use of technology we should have to look at three important points, those are victim privacy, surveillance and free speech against TFGBV.

6.1 Privacy of victim

The idea of privacy is not a modern concept; it dates back to the earliest human civilizations. Privacy is regarded as one of the fundamental right of individuals; this is why it is protected by law in every state. No one is allowed to intervene your privacy, and if they do, you have right to take legal action. Privacy rights are also safeguarded by international law, such as the International Covenant on Civil and Political Rights ICCPR, ICESCR, etc.

United nation charter also protects right of privacy under the article 18:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Many apps and technologies are not end-to-end encrypted, which is alarming and rise in need of an ethical responsibility of app developers to ensure the security level of its users. Access by third party in these apps should be prohibited. In most of cases, image based abuse happen due to the unethical access to third party. Same happen for deepfake when they use them to blackmail the users.

Different countries are take various steps for protection of their citizens in this digital age as in New York it is prohibited to install cameras in hotel rooms and bathrooms as well and in California two way mirrors are also banned. (DeVries, Protecting Privacy in the Digital Age).

6.2 Free Speech in addition to Harmful Online Content

Free speech means you have freedom to express your ideas. Freedom of speech is considering one of basic right of all over world except few countries like North Korea. On social media platforms there is very thick line between free speech and the harmful content spread online through this. For instance, most of people begin to spread misinformation just because of this right as in May, 2023 an AI synthesized fake visual of Pentagon explosion through verified account on social media platform X formerly known Twitter, which spread misinformation among people and there was fear among people. (Haddad, 2023)

Right of free speech should be exercise but it must come with certain boundaries. There should be some restrictions for the sake of preventing the spread of misinformation, and aggressive speech should be banned. Abusive language must be prohibited under every circumstance. Virtual harassment, under umbrella of "free Speech" should not be tolerated by anyone.

6.3 Digital evidence

In modern age there are various tools and technologies, which can be used to identify that whether the video, audio or text through harassment or abuse taken place is whether authentic or not. For instance, if anyone uploads a deepfake of someone else through a faked account and through which blackmailing occur. The account could get access through this evidence and after that legal action can be taken against the perpetrator.

Today, camera footage (CCTV) can be used in most of the crimes. In addition to this digital evidence in stalking also could be used and if hackers get access to someone's account the messages and the content which has been uploaded from this account through this also get access against the hackers. Videos or image detector of AI generated videos can also be used as a digital evidence to detect that whether the content is original or fake in especially violence of image abuse and the violence through deepfake which have been very common in these days.

App developers should keep rule of confidentiality under which the data of user is not accessible to anyone else and also have to follow the Data Minimization Principle under which collection of user's data which is necessary to regulate or for functionality of app, through the consent of users.

7. Role of international agreements and conventions in combating TFGBV

International agreements and conventions do play an essential role in combating with TFGBV by providing standard definitions of the TFGBV, what constitutes TFGBV and ways to control it. The question that arises here is that does the ratification of International treaties make state parties compliance bound and do these international treaties create domestic pressure or not?

The primary source in international law is international treaty ratified by states. These states subject to these treaties are required actions not to violate the provisions of treaty. ICCPR forbids gender discrimination. In ICCPR, prohibition of "inhuman and degrading treatment" impliedly means the prohibition of gender based violence.

CEDAW is a breakthrough in establishing women rights. Its ratification has been done by 189 states. This convention provides that states should not legislate any laws which violate rights of women and these state parties are also required any such existing law which serves as a discrimination towards women. Article 2 of the CEDAW states that:

"To take all appropriate measures, including legislation, to modify or abolish existing laws, regulations, customs and practices, which constitute discrimination against women."

The later recommendations made by CEDAW committee have included violence against women in definition of "discrimination". (Convention on the Elimination of All Forms of Discrimination Against Women, 1979) The Committee's General Recommendation No. 19 (1992) has incorporated Gender Based Violence in the concept of discrimination. It refers to not only physical harm but mental or sexual mistreatment also. (Convention on the Elimination of All Forms of Discrimination Against Women, General Recommendation No. 19, 1992) It also provides that States can also be accountable if they fail to take action against violations of rights or even if they fall short in investigation and providing punishment in cases of violence.

From 2004 till 2015 CEDAW has issued 32 decisions in total addressing gender-based violence. For example, it has in its 32nd session found that Hungary violated the CEDAW because it failed to provide "protection meeting international standards in cases of domestic violence" (Views of U.N. Committee on the Elimination of Discrimination Against Women, 2005)

CEDAW provides the opportunity of Shadow Reports to women and organizations to highlight any gaps between the ratification and compliance of the convention.

The Budapest Convention on cybercrime has further provided special protection for women suffering from OGBV. It is regarded as first treaty at international level providing protection for online crimes against women. It mainly concerns exploitation images, child obscenity for distribution in electronic world. (Anadaru, 2021)

The Istanbul Convention is a legally binding human rights treaty that covers all forms of violence against women particularly addressing online and technology facilitated violence against women.

The Istanbul Convention and the Budapest Convention work together in addressing various aspects of violence. The Istanbul Convention focuses on the sex-specific attributes of violence done against women, while the Budapest Convention provides operational tools and fosters cross-border cooperation to combat offenses involving electronic evidence. These connections were explored in a T-CY Cyber violence mapping study, as well as in the report "Protecting Women and Girls from Violence in the Digital Age," authored by international consultant Adriane van der Wilk under the direction of the Council of Europe's Violence against Women Division.

Furthermore, the European Union stresses the significance of OGBV through measures that protect vulnerable group namely, the Directive on Victims' Rights, Victim Rights Guide, Guidelines on Prevention and Eradication of Trafficking in Persons and Efforts to Protect Victims and Guidelines for Combating Sexual Exploitation of Children Online and Child Pornography. (Human Rights Council Thirtieth Session Agenda number 3, 2016).

8. Recommendations

Conducting research aiming to understand the rapid increase of the dynamics of violence and how it can be dealt with the changing of AI. It can be done by recruiting local research team and collaboration between them and non- local research teams.

Low levels of this awareness are serving as an obstacle to address the issue of TFGBV. For those organizations that plan to implement new TFGBV programs involving public awareness can engage with organizations already working on it. For example: at international level they can collaborate with

Sexual Violence Research Initiative (SVRI), UNFPA, and the Global Partnership for Action on Gender Base Online Harassment and Abuse.

The current legislation against TFGBV has significant gaps and doesn't provide the full coverage of the TFGBV spectrum. To deal with it country level experts in the field of law as well as in the field of AI should come together to review the current legislation and make required recommendations about changes needed to be made in law and how other legislative tools along with AI can be used to combating against TFGBV. Proposing the policies for instance content moderation etc. that AI can detect and automatically report it to the authorized institutions can help with the erasure of TFGBV.

If access to data is mandatory, it should be limited to data that has been consented, which is regulated by AI (Automated access control).

The current reporting mechanisms are very limited that has failed to lead prosecution. Also these mechanisms bring financial burden on TFGBV survivors that's why survivor are not able to use these mechanism effectively having a survivor centered approach in reporting mechanisms whether online or offline can deal with TFGBV cases productively. Social media and tech companies should also ensure that there reporting mechanisms are up-to-date and incompliance with global and national protections against TFGBV for instance UN's policy brief on information integrity on digital platforms publishing in 2023. There is also requirement of mechanism to holding perpetrators accountable.

The advancement of technology has not only facilitated patriarchal narratives but also the oppression of vulnerable groups of society. Therefore, it has now become a threat against gender equity movement. It is of importance that the future TFGBV programming must include up-to-date knowledge and strategies to deal with this challenge. Using a gender transformative approach aimed to transform the primary causes of gender inequality in societal norms, roles, practices and legislation. For example International Alert is an organization recommended calling on all stakeholders to address the issue of patriarchal norms.

9. Conclusion

This study has explored a global issue of TFGBV and its impact on public. The findings emphasize the urgent need for sturdy legal framework and public policies that provide a shield against TFGBV and protect victims as well. AI tools such as machine learning, algorithms and other monitoring, and detecting tools that can use to prevent online abuse. AI helps to identify deepfakes or harmful behavior and hate speech in online discussion. Along with these AI tools, International and national legislation also exist to address the issue of TFGBV but the use of AI in the laws to combat against TFGBV is underdeveloped area and is still evolving. This study highlights that the ethical considerations around surveillance, data privacy and digital evidence must be managed carefully. Collaboration between AI developers and law makers is essential to combat against TFGBV and ensuring the fundamental rights of users. Some international agreements and conventions for example Budapest convention has recognized the need of more TFGBV targeted legislation.

References

(2019). Retrieved from UNESCO.

(2020). *IWF Annual Report 2020 - Face the Facts.* Internet Watch Foundation.

(n.d.). Retrieved from Dawn.

(n.d.). Retrieved from UNESCO: https://unesdoc.unesco.org/ ark:/48223/pf0000384920

(n.d.). *Still We Dream.* Plan International.

(n.d.). UNESCO.

(n.d.). UNESCO.

AI and Gender-Based Violence. (2024, August 30). Retrieved from Dawn: https://www.dawn.com/news/1855645

Anadaru, I. P. (2021). Cyber Child Grooming Sebagai Bentuk Kekerasan Berbasis Gender Online Di Era Pandemi. *Jurnal Wanita Dan Kaluarga*, 41-51.

Artificial intelligence, toward new horizons in the fight against gender-based violence. (n.d.). Retrieved from USAID: https://infosegura.org/en/blogs/artificial-intelligence-toward-new-horizons-fight-against-gender-based-violence

Basic Online Safety Expectations: Regulatory Guidance . (n.d.). Retrieved November 2024, from esafety commisioner: https://www.esafety.gov. au/sites/default/files/2024-07/Basic-Online-Safety-Expectations-regulatory-guidance-July-2024.pdf.

Communication, D.-G. f. (2024, Aug 1). *AI Act enters into force*. Retrieved from European Commission: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

Convention on the Elimination of All Forms of Discrimination Against Women, General Recommendation No. 19. (1992). U.N. Comitte in the Elimination of Discrimination Against Women .

DeVries, W. T. (n.d.). Protecting Privacy in the Digital Age.

Digital Services Act-Consilium. (n.d.). European Council.

Evon Abu-taieh, A. A. (2019, January). Cyber Security Crime and Punishment: Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia.

Gernort Fritz, T. E. (2024). Eu AI Act unoacked #8: New rules on deepfakes. Lexology.

Gomez, A. (2024, Apr 25). Cybersecurity Ethics: Everything You Need To Know. OLLU.

Haddad, M. (2023, May 23). Fake Pentagon explosion photo goes viral: How to spot an AI image. AlJazeera.

Herring, S. (2002). Cyber Violence: Recongizing and resisting abuse in online enviroments. . Asian Women.

Human Rights Council Thirtieth Session Agenda number 3. (2016, July 1). *Resolution adopted by the Human Rights Council*.

Janine M. Zweig, M. D. (2013, July). TECHNOLOGY, TEEN DATING VIOLENCE AND ABUSE, AND BULLYING. Washington, DC: Urban Institute.

Kelly, M. (2023, May 2). *Democrat sounds alarm over AI-generated political ads with new bill*. Retrieved from The Verge: https://www.theverge.com/2023/5/2/23708310/ai-artificial-intelligence-political-ads-election-rnc-biden

L. Hinson, J. M.-M. (2018). Technology-facilitated Gender-based Violence: What Is It, and How Do We Measure it? (Washington D.C.: International Center for Research on Women). . Washihngton DC: International Center for Research on Women.

Landscape Analysis of Technology-Facilitated Gende-Based Violence: Findings frim Asia. (2022). NORC at the University of Chicago, International Centre for Research on Women (ICRW).

Making Britian the Safest place in the world to e online . (2017, Oct 11). UK Government.

Malanga, D. (2020, August 19). Tackling Gender-Based Cyber Violence against Women and Girls in Malawi Amidst the COVID-19 Pandemic. University of Cape Town (UCT); University of Livingstonia.

Monica Anderson, J. J. (2018). *Teens, Social Media and Technology 2018.* Pew Research Center.

Morris, S. (2023, May 23). *AI-generated Pentagon explosion image was shared by verified Twitter accounts*. Retrieved from The Standard: https://www.standard.co.uk/news/tech/ai-generated-pentagon-explosion-attack-image-viral-twitter-b1083152.html

Posetti, J. S. (2021). The chilling: Global trends in online violence against women journalists. UNESCO.

Protection from Harassment Act. (2011). Government of South Africa.

Regulatory Information. (n.d.). Retrieved November 2024, from esafety commisioner: https://www.esafety.gov.au/industry/regulatory -information.

Ruth Lewis, M. R. (November 2017). *The British Journal of Criminology, Volume 57, Issue 6*.

Ruth Lewis, M. R. (2016). Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls. *The British Journal of Criminology*.

Sarah, F. (2022, December 11). TPKS Bill Ratified to Law: Implications on Indonesia's Online Sexual Violence Status Quo. Indonesia: Center for Digital Society.

Sharp rise in violence against women and children in Sindh during 2023. (2023). Sunstainable Social Development Organization.

Technology-Facilitated Gender-Based Violence Program (TFGBV) Globally. (2023, January 17). Retrieved from US Department of State.

The online crisis facing women and girls threatens global progress on gender equality. (2020). The World Wide Web Foundation.

UN-Women, Accelerating efforts to tackle online and technology facilitated violence against women and girls (VAWG). (2022). UN.

Vaiddehi Bansal, M. R. (2022, Feburary). LANDSCAPE ANALYSIS OF TECHNOLOGY-FACILITATED GENDER BASED VIOLENCE. ICRW, NORC.

Van Der Wilk, A. (2018). Cyber Violence and hate speech online against women: Study. European Parliament.

Views of U.N. Committee on the Elimination of Discrimination Against Women. (2005, Jan 26).

Werner, J. (2024, Sep 9). *Pakistan Senate Proposes AI Regulation Bill with Heavy Penalties*. Retrieved from babl: https://babl.ai/pakistan-senate-proposes-ai-regulation-bill-with-heavy-penalties/#:~:text=The%20%E2%80%9CRegulation%20of%20Artificial%20Intelligence%20Act%202024%E2%80%9C%20is%20designed%20to,collection%20and%20safe%20AI%20systems.

What is gender-based violence? (n.d.). Retrieved from European Comission: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/gender-equality/gender-based-violence/what-gender-based-violence_en

Women In The Spotlight. (n.d.). Retrieved November 2024, from esafety comissioner: https://www.esafety.gov.au/women/women-in -the-spotlight