Online Gender-Based Violence and Artificial Intelligence

Cynthia Ojukwu

De Montfort University, Leicester

ABSTRACT

There are positive and negative impacts of artificial intelligence on human rights today. These impacts are not equally distributed in our societies. Some people and some groups are affected more strongly than others whether positively or negatively. Narrowing this discussion to how AI affects women and girls, this paper identifies a deep connection between digital authoritarianism affecting women and girls and online gender-based violence. Unfortunately, this is the new category of gender-based violence. There should be galvanised efforts to incorporate into international human rights law, and regional human rights law this new category of crime known as online gender-based violence. Efforts should be made to criminalise online gender-based violence, including AI-created abuses and deepfakes targeting women and girls. This paper considers whether existing EU AI legislation provides criminal law mechanisms for punishing online gender-based violence. Other regions of the world such as Africa need to join deliberate efforts to protect women and girls from online gender-based violence. Additionally, this paper considers whether Africa has a regional framework for criminalising online gender-based violence in the region. From an intersectional viewpoint, this paper implores on state actors and non-state actors to recognise the interconnection between AI and gender. It also points to future research directions for further study of online gender-based violence which should be considered for policymaking. Finally, this paper highlights some possible roles criminal law can play in mitigating online gender-based violence against women and girls, so it would not lead to another global pandemic.

Introduction

Technology facilitated gender based violence (TFGBV) mirrors and aggravates existing forms and patterns of gender based violence (GBV). This includes intimate partner violence (IPV), political violence, and new forms and patterns of GBV which have emerged that can only take place through technology and online spaces.[1] Some of them include image based abuse through artificial intelligence (such as sexual deepfake videos or virtual reality pornography). Most importantly, Artificial Intelligence (AI) negatively impacts diverse communities in various ways.[2] These negative impacts of AI towards women and girls constitute the main discussions of this paper.

[1] Suzie Dunn, 'Technology-Facilitated Gender-Based Violence: An Overview supporting a safer internet Paper' (2020) 1 Centre for International Governance Innovation assessed 28/04/2025

[2] Ibid

Technology facilitated gender based violence is a comprehensive term that includes any act of gender based violence that is perpetrated, assisted, or amplified using technology, while cybercrime refers to criminal acts committed using technologies.[3]

Although, cybercrime and TFGBV differ, there is an overlap between them and so throughout this paper they are used to mean the same thing particularly as they affect women and girls.

It is widely recognised that artificial intelligence has been progressively transforming the world and impacting our lives significantly. This transformation goes together with the promise that AI exists to improve our lives. However, there are downsides that considerably impact our lives negatively. Unfortunately, it appears there is greater focus on the transformation of AI to improve our lives than on the existing patterns of bias and discrimination which AI perpetuates. In fairness, several efforts have been made towards improving the ethics of AI.[4] While focusing on how the ethics of AI is crucial for operational improvements and the reduction of human error, ongoing dialogues should expand to consider the human rights and legal implications of these technologies.[5] This paper's contribution provides value by synthesizing and integrating the literature across related areas and research studies.

Online gender-based violence affects women and girls differently in varied circumstances. Recently, research focus has shifted towards authoritarian leaders who maintain power and control by defending a patriarchal social order and mobilising against feminist ideas. Women human rights defenders, politicians and journalists in authoritarian governments face gendered forms of digital threats that exploit their gender identity to intimidate, shame and discredit them.[6] These gender-based digital transnational repression extends forms of authoritarian domination from domestic and "offline" settings into digital space and the transnational field.[7] Transnational repression is understood as an extension of domestic political controls, reproducing the coercive power of the authoritarian state outside its territorial boundaries.[8]

Michaelsen et al. reveal some of the dynamics of technology-facilitated gender-based violence.[9] This form of GBV shows that digital technologies reproduce, extend and intensify offline harassment, abuse and other forms of violence into online space. Women who are seen to question male privilege or unsettle gender stereotypes are most likely to face a severe backlash in the form of "identity-based digital attacks. As a result of that, these women experience economic, professional, and psychological harm.

---

[3] Ibid

[4] Filippo A. Raso, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, and Levin Kim, 'Artificial Intelligence & Human Rights: Opportunities & Risks', 2018 The Berkman Klein Center for Internet & Society Research Publication Series

[5] Ibid

[6] Marcus Michaelsen and Siena Anstis, 'Gender-based digital transnational repression and the authoritarian targeting of women in the diaspora,' 2025 *Democratisation* Routledge

[7] Ibid

[8] Ibid

[9] Ibid

Technology facilitated gender based violence is recognised as a form of discrimination. This form of discrimination negatively impacts a range of human rights, including the right to a life free from violence, the right to privacy, the right to freedom of expression, the right to participate in public and political life, and the right to access and use digital technologies.[10] This online violation of women's rights is a violation of their fundamental human rights and so, it is a human rights issue.[11] While this paper recognises everyone's rights to freedom of expression, there is need to protect the rights of women and girls in the digital space.

From the human rights perspective, the recent 2024 Report of the UN Secretary-General identified the growing backlash against women's rights, the rapid rise of Artificial Intelligence (AI) and the expansion of the manosphere as emerging challenges in this digital era.[12] This paper refers to this vice as either technology facilitated violence against women and girls (TFVAWG), technology facilitated gender based violence (TFGBV) or cybercrime.

This Report defined technology-facilitated violence against women and girls (TFVAWG) as any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms.[13] Forms of TFGBV are wide and varied, and, like other forms of GBV, can be sexual, emotional, psychological, economic, and can result in physical and psychological harm.[14] Other forms of TFVAWG include defamation, violent threats, astroturfing, misinformation, hate speech, doxing, impersonation, cyber-harassment, hacking and stalking, image and video-based abuse.[15] Further, this Report identified that while all women and girls are at risk, some groups are disproportionately affected.[16] Women in the public eye and marginalised women and girls continue to be most affected by TF VAWG.[17] Although this paper identifies these groups as affected by this problem, any woman and girl in the digital space is likely to suffer online GBV. According to the paper from the Global Partnership, a government-to-government body, launched at the 66th session of the Commission on the Status of Women in March 2022, 20% of women

[10] UN Human Rights Council (2016). The promotion, protection and enjoyment of human rights on the Internet, Resolution adopted by the Human Rights Council on 1 July 2016. A/HRC/RES/32/13. <https://www.refworld.org/ docid/57e916464.htm> assessed 28/04/2025

[11] United Nations Human Rights Office of the High Commissioner, '"Digital rights are human rights:" Women activists fight cybersexism,' 2024, OHCHR

[12] UN Women, 'FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women' 2025 <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women> assessed 12/03/2025

[13] Ibid

[14] UN Human Rights Council, 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective', 2018, 38th session < https://digitallibrary.un.org/record/1641160>

[15] UN Women (n12)

[16] Ibid

[17] Ibid

journalists participating in a UNESCO global survey said that offline attacks were directly linked to online violence targeting them.[18]

Similarly, a UN empirical research found that 73% of survey participants identifying as women and recruited for the study, have experienced online gender-based violence.[19] This same study recorded threats of physical violence (identified by 25% of survey respondents) including death threats, and sexual violence (identified by 18%) also plagued the women journalists that were interviewed.[20] Also, 13% of survey respondents and many interviewees said they had received threats of violence against those close to them, including children and infants.[21] One-fifth (20%) of survey respondents identifying as women said they had been attacked or abused offline in connection with online violence they had experienced.[22] Further, the report from the UN Broadband working group reveals that women are 27 times more likely to be abused online than men.[23] The Report also shows that 61 per cent of online harassers are male, and that women aged between 18 and 24 are at particular risk.[24]

Part of the UN efforts revealed that the UN General Assembly adopted the first ever UN General Assembly Resolution on Artificial Intelligence (AI) for Sustainable Development.[25] Five months later, in August of 2024, the United Nations approved the draft of a historic global cybercrimes treaty, coined the United Nations Convention Against Cybercrime.[26] On December 24, the UN General Assembly adopted this landmark convention on "Countering the use of information and communications technologies for criminal purposes," otherwise known as the cybercrime convention.[27] The UN cybercrime treaty is poised to become the seminal global legally binding instrument on cybercrime as announced by the UN Office on Drugs and Crime (UNODC).[28] This process marked the first time that UN member states have begun to negotiate a legally binding treaty on cyber-related issues.[29]

---

[18] The Global Partnership, 'Technology Facilitated Gender Based Violence Preliminary Landscape Analysis,' 2023, Social Development Direct
[19] UN Women (n12)
[20] Ibid
[21] Ibid
[22] Ibid
[23] United Nations Broadband Commission for Digital Development Working Group on Broadband and Gender (2015), Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call, available at <www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violene_gender%20report.pdf >assessed22/04/2025
[24] ibid
[25] United Nations Office for Digital and Emerging Techs., Global Digital Compact, U.N. OFFICE OF THE SECRETARY-GENERAL'S ENVOY ON TECHNOLOGY., U.N. Doc. A/79/L.2 (Sept. 22, 2024)
[26] Press Release, United Nations Office on Drugs & Crime, Member States Finalize a New Cybercrime Convention, U.N. Press Release (Aug. 9, 2024), <https://www.unodc.org/romena/en/press/2024/August/press-release_-united-nations_- member-states-finalize-a-new-cybercrime-convention.html>
[27] Rangita de Silva de Alwis, 'Gendering the New International Convention on Cybercrimes and New Norms on Artificial Intelligence and Emerging Technologies',2025, Washington Journal of Law and Technology
[28] Jule Pattison-Gordon, United Nations Approves Draft Global Cyber Crime Treaty, GOV'T TECH. (2024), <https://www.govtech.com/security/united-nations-approves-draft-global-cyber-crime-treaty>
[29] Rangita de Silva de Alwis (n27)

In 2024, ahead of the Summit of the Future, the Secretary General introduced his Agenda for Peace, committing to "transforming the gendered power dynamics in peace and security.[30] Against the backdrop of the UN Charter and pushbacks against human rights, particularly women's rights, the New Agenda for Peace highlights significant global challenges.[31] Among these are the potential weaponization of new technologies against women and the consequent rising inequalities.

Following the growing trend of online gendered crime, this paper discusses and analyses legal interventions targeting online gender-based violence as a technology facilitated violence against women and girls. Notably, AI and technology are used interchangeably but are not the same, although AI is a part of technology. To maintain scope, this Paper focuses on how AI as a part of technology has negatively impacted the rights of women and girls. Hence, online gender-based violence, technology facilitated, and AI facilitated violence against women are used interchangeably in this Paper.

This paper is structured in a way that following the introductory remarks, the next section defines concepts. After that, the following section identifies and discusses the interconnection between artificial intelligence and gender. Sections following this, analyse AI and human rights, consider whether existing EU AI legislation provides criminal law mechanisms for punishing online gender-based violence and how other regions such as Africa can be brought up to speed regarding this pandemic. International law interventions are also analysed leading to the provision of some recommendations as a call for possible roles criminal law can play in mitigating online gender-based violence against women and girls, so it would not lead to another global pandemic. Galvanised efforts are required to incorporate into international human rights law, and regional human rights law this new category of crime known as online gender-based violence. Some concluding remarks form the last section of this Paper. Throughout this Paper, artificial intelligence is referred to as AI.

Definition of Concepts

The UN Special Rapporteur on violence against women back in 2018 defined online gender-based violence as 'Any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.[32] Additionally, this section attempts to define AI, gender and technology as separate terms. Regarding the definition of AI, there is no widely accepted definition of AI, however Artificial intelligence can be defined as the study of making computers do things which, at the moment, humans do

[30]U.N. Secretary-General, Our Common Agenda Policy Brief 9: A New Agenda for Peace, 15, (July 2023) <https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-new-agenda-for-peace-en.pdf >
[31] Ibid
[32] Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47, 2018

better.[33] AI may also be defined as creating a computer process that acts in a manner that an ordinary person would deem intelligent.[34] In simple terms, AI refers to machines that mimic human intelligence. Artificial Intelligence is part of technology. Therefore, as earlier mentioned in the introduction section of this work, this paper focuses on how AI as a part of technology has negatively impacted the rights of women and girls. Technology encompasses a broader range of tools and systems which include hardware, software, and networks.[35] Technology includes everything from simple tools like hammers to complex systems like computers, the internet and smartphones.[36] Technology aims to solve practical problems and improve efficiency.[37] By helping to solve practical problems and improve efficiency, this critical role of technology diverts attention from the negativity it also offers.

Artificial Intelligence and Technology Facilitated Gender-Based Violence

It is important to note that AI creates a significant and complex influence on technology facilitated gender-based violence. AI systems are trained on vast datasets and where these datasets contain historical and societal biases, the AI will learn and perpetuate them.[38] This can lead to algorithms reinforcing gender stereotypes, discriminatory recruitment practices, and inadequate medical treatment for women.[39] The underrepresentation of women in AI development further exacerbates this issue, leading to predominantly male perspectives guiding AI's decision-making processes.[40] As a form of AI, generative AI is wrongly used by perpetrators of online GBV against women and girls in the online space.

Generative AI as a form of AI enables the creation of highly realistic deepfakes otherwise known as manipulated images or videos often pornographic and non-consensual which disproportionately target women.[41] In simple terms, generative AI offers a generative model of AI capable of producing texts, images, or programming code.[42] These deepfakes are used to depict individuals in situations they never consented to, and generative AI has made it easier and more realistic to create deepfakes.[43] This non-consensual

---

[33] Asa B. Simmons and Steven G. Chappell, 'Artificial Intelligence-Definition and Practice', (1988), 13 IEEE Journal of Oceanic Engineering 2

[34] Damodar Singh Rajpurohit and Rishika Seal, 'Legal Definition of Artificial Intelligence', (2019), 10 Supremo Amicus 87

[35] AI Tech Café, 'What is the Difference between AI and Technology?' 2024, <https://www.bing.com/ck/a?!&&p=90df3d47197d3da6b700442e74fb9d5a7e05cd6dce717f6bc67e71dbd79600d8JmltdHM9MTc0NDMyOTYwMA&ptn=3&ver=2&hsh=4&fclid=07ec8468-1bfa-6fb0-076f-97161a566e65&psq=is+technology+same+as+artificial+intelligence&u=a1aHR0cHM6Ly9haXRlY2hjYWZlLmNvbS93aGF0LWlzLXRoZS1kaWZmZXJlbmNlLWJldHdlZW4tYWktYW5kLXRlY2hub2xvZ3kv&ntb=1> assessed 11/04/2025

[36] Ibid

[37] Ibid

[38] UN Human Rights Council (n14)

[39] Ibid

[40] Ibid

[41] Beatriz Kira, 'When non-consensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act,' 2024 Computer Law & Security Review 54

[42] Leonardo Banh and Gero Strobel, 'Generative Artificial Intelligence', 2023 *Electron Markets* 33

[43] Beatrice Kira (n41)

dissemination of intimate images is a severe form of TFGBV. Many AI models are developed without adequate safety measures built in from the outset, increasing the risk of their misuse for TFGBV.

Connection between Gender, Artificial Intelligence (AI), and technology facilitated violence against women and girls.

Artificial Intelligence has provided platforms for acquiring new powers and abilities for using technology for online GBV against women and girls. The weaponization of technology is part of the continuum of assault on women's rights both online and offline and so, like all forms of GBV, TFGBV is driven by structural gender inequality.[44] Gender-based violence happening online is representative of the history of gender-based violence in the society. While the online-offline distinction is often blurred, the online sphere offers a space for anonymity, and geographic distance, thus providing a veil of impunity for the offenders.[45]

From the UN studies captured in the introduction section of this work, this paper identifies a connection between gender, artificial intelligence and people (such as women and girls) who face intersecting systemic forms of discrimination and oppressions. Although, this connection is largely ignored, this paper suggests that this form of violence is targeted at women and girls mostly by reason of their gender. To establish this connection, scholars such as Marganski and Melander identify that gendered cyberhate has become common in digital spaces, and behaviours comprising it have grown increasingly threatening to recipients particularly women and girls.[46]

With an intersectional perspective, this paper understands that this growing online crime affects women and girls from varying backgrounds in different ways. This paper also identifies it as a phenomenon which is deeply connected with the historical subordination of women and systemic violence against them in society.

As severally mentioned, women and girls with different characteristics and backgrounds experience TF GBV in different degrees and in different ways.[47] Accordingly, Sobieraj observes, that these online attacks are particularly severe for (1) women who are members of multiple marginalized groups, (2) those who are speaking publicly in or about male-dominated spheres, and (3) women who are perceived as feminist or noncompliant

[44] The Global Partnership (n18)
[45] Rangita de Silva de Alwis (n27)
[46] Alison J. Marganski, Lisa A. Melander, 'Technology-Facilitated Violence Against Women and Girls in Public and Private Spheres: Moving from Enemy to Ally,' (eds. Alison J. Marganski and Lisa A. Melander) in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Insight 2021)
[47] United Nations Development Programme, 'Analysis of the legislation related to Technology Facilitated Gender Based Violence', 2024 UN Publications <https://www.undp.org/sites/g/files/zskgke326/files/2024-12/final-analysis-tf-gbv.pdf>

with traditional gender norms.[48] For example, women who engage in public debate through the internet, are susceptible to a high risk of harassment experienced online.[49]

These online GBV behaviours include sexually violent invective, plausible rape and death threats, stalking, large groups attacking individuals, the malicious circulation of targets' personal details online ('doxing'), and the uploading of sexually explicit material without the consent of the pictured subject ('revenge porn').[50] In some cases, these online attacks involve offline dimensions for instance, doxing, which is often accompanied by incitements to internet antagonists to hunt targets offline.[51] Gender-based violence against women online also communicates a sense of outraged objectification of women's bodies that is not separate from – but rather a continuation of – offline activities.[52] Notably, this reveals the relationship between the offline and online realms of these gendered crimes and how they transcend the online realms of abuse and violence against women and girls to offline realms and vice versa.

Data breaches such as those experienced in Brazil and Chile may also carry differentiated offline gendered impacts. For example, in cases where breaches of medical data are exposed, the personal information of women, especially in relation to reproductive care, might have harmful gendered consequences.[53]

Providing some context for this gendered violence and abuse online-offline connection to be easily identified, this pull-quote shows how online gender-based abuse can be used against women and girls:

> *she displeases him and he tries to punish her. He posts doctored photos of her to the web. In one, a noose is near her head. In another, her children appear to be performing sex acts. He emails graphic threats about violating her with a chainsaw. He sneers that she is too fat to be loved, and then — missing the irony — calls her a slut. He distributes her Social Security number online. He posts lies about a prostitution bust. Posing as her, he solicits sex in online ads and includes her home address, so men knock on her door at all hours. Maybe he's anonymous but often he doesn't bother hiding his identity.*[54]

---

[48] Sarah Sobieraj, 'Bitch, Slut, Skank, Cunt: Patterned Resistance to Women's Visibility in Digital Publics' (2018) Information, Communication & Society, <doi:10.1080/1369118X.2017.1348535>.
[49] United Nations Development Programme (n47)
[50] Emma A. Jane, 'Feminist Flight and Fight Responses to Gendered Cyberhate', in *Gender, Technology and Violence* (Routledge 2018)
[51] Greg Sandoval, 'The end of kindness: Weev and the cult of the angry young man', (2013)
The Verge, available at< www.theverge.com/2013/9/12/4693710/ the-end of-kindness-weev-and-the-cult-of-the-angry-young-man >(accessed 22 Apr. 25).
[52] Stella marina Donato, Hande Eslen-Ziya, and Emiliana Mangone, 'From offline to online violence: new challenges for the contemporary society,' (2022), 32 International Review of Sociology 3
[53] Women in Global Health, HER STORIES: ENDING SEXUAL EXPLOITATION, ABUSE, AND HARASSMENT OF WOMEN HEALTH WORKERS (2022), <https://womeningh.org/wp-content/uploads/2022/12/WGH-Her-StoriesSEAH-Report_Policy-Report-Dec-2022>assessed 19 May 2025
[54] Stella marina Donato et. al (n52)

The above quotes representing possible scenarios clearly explain the connection between gender, online GBV and artificial intelligence. To tackle and reduce the possible occurrences of the above scenarios happening to real women and girls, this paper argues that there is need to formulate a shared language and global infrastructure around which different stakeholders can engage. When nations adopt and implement this shared global legislation, it then creates an enabling transnational environment that fosters a multi-stakeholder approach. Hence this question arises: how has international law offered a significantly proportionate response to online GBV.

In consideration of the connection between online GBV, AI and gender, it is relevant to mention that the traditional understandings of violence including gender based violence tend to prioritise physical acts.[55] This paper suggests that less attention given to online gender-based violence may have originated from the lasting idea that only physical injuries or acts are considered crimes. Although the direct physical act of gendered violence and sexual violence are different from online violence, there are similarities between these forms.

Women and girls with multiple intersecting identities experience online GBV in peculiar ways. These acts share the structural gender and intersectional inequities that lie at the root of such conduct. These intersectional inequities could be race and gender, disability and gender, economic status and gender as well as sexual orientation and gender. For example, women from different races particularly those from the Black, Asian Ethnic Minority (BAME) group may experience a unique form of online GBV that combines racism and misogyny. Women and girls from varied sexualities and races experience discrimination and abuse based on both their sexual orientation and gender. Women with disabilities are also not exempted from this discrimination.

One could possibly argue that women and girls are free to leave an abusive online environment, however, this response denies their right to assembly and expression in the online public square.[56] In addition to denying their right to assembly and expression, this paper identifies that it reinforces power inequalities in the online and offline space.

According to Jane, this technology facilitated GBV crimes have the potential to cause emotional, social, financial, professional and political harm to women and girls.[57] Therefore, it becomes imperative to interrogate whether 'AI facilitated gender-based violence is the next pandemic and what are the legal frameworks available to combat this growing global trend and pattern?'[58]

Legal Framework on Technologically Facilitated Violence against Women and Girls

[55] Alison J. Marganski et. al (n46)
[56] Rangita de Silva De Alwis, 'A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence', (2024) LA REVUE DES JURISTES DE SCIENCES PO 25
[57] Emma A. Jane (n50)
[58] Rangita de Silva de Alwis and Elodie Vialle, 'Is AI-Facilitated Gender-Based Violence the Next Pandemic?', 2024, University of Pennsylvania Carey Law School <https://www.law.upenn.edu/live/news/16727-is-ai-facilitated-gender-based-violence-the-next>

Part of State parties' responsibility towards women and girls is to provide full protection to women and girls from online gender-based violence as well as create and implement legal framework, policies and measures against it. In line with that, the UN Special Rapporteur on Violence against Women further stressed that,

> "States should adopt or adapt (as appropriate) their criminal and civil causes of action to hold perpetrators liable" and, in particular, "clearly prohibit and criminalise online violence against women, in particular, the non-consensual distribution of intimate images, online harassment and stalking".[59]

Presently, there is no consensus across countries on how to regulate online content.[60] Emerging evidence suggests that there are gaps in legislation and inconsistency in implementation of some existing criminal laws in dealing with different forms of TFGBV.[61] Organizations like Equality Now are working on model laws to guide states in implementing comprehensive measures for TFGBV. [62]

The globally recognised European Union Artificial Intelligence Act, (EU-AI Act) has been formulated as a guidance for further enactments in this area. Notably, despite Brexit, the Act will be crucial to the UK AI industry's aspirations as exporters to the EU or providers of 'AI-as-a-Service'.[63] Article 3 of the Act states that providers of systems who develop an AI system with a view to placing it on to the market or putting it into service under their own name or trademark are subject to obligations under the Act.[64] Clearly, this Act is not specifically aimed at combating AI facilitated GBV against women and girls. To fill this gap created by this legation formulated in 2021, the European Union adopted the Directive on violence against women and domestic violence, marking the first EU-wide binding legislation to address various forms of sexualized and gendered harm.[65] This Directive provides for image-based sexual abuse ("IBSA"), encompassing the non-consensual taking, creating, and sharing of intimate materials, as well as threats to distribute them.[66]

---

[59] The report of the UN Special Rapporteur on Violence against Women on the Causes and Consequences on online violence against women and girls from a human rights perspective can be found on the following link:< https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteurviolence-against-women-its-causes-and consequences on online violence against women and girls from a human rights perspective> assessed 24/04/2025

[60] Ibid

[61] The Global Partnership (n17)

[62] Equality Now, 'Advancing a Model Law on Technology-Facilitated Gender-Based Violence,' (2024), News and Insights, Equality Now < https://equalitynow.org/news_and_insights/advancing-a-model-law-on-technology-facilitated-gender-based-violence/> assessed 20/04/2025

[63] Jennifer Cobbe, Jatinder Singh, 'Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges.' (2021) Computer Law and Security Review, volume 42. Available at: <https://www.sciencedirect.com/science/article/pii/S0267364921000467> assessed 28/04/2025

[64] Lilian Edwards, 'The EU AI Act: a summary of its significance and scope', *Artificial Intelligence: (The EU Act)* 1 (2021)

[65] Carlotta Rigotti, Clare McGlynn and Franziska Benning, 'Image-Based Sexual Abuse and EU Law: A Critical Analysis,' 2024, German Law Journal, Cambridge University Press

[66] Ibid

In as much as these are landmark progresses, Rigotti et al. recognise that these legislations do not capture the full spectrum of the issue.[67] This paper aligns with this assertion, more so as AI continues to advance while victims continue to suffer a wide range of emotional, psychological, professional, and relational adverse effects. To date, the main challenge lies in effectively overseeing and enforcing existing regulations, as well as making necessary adjustments to address this evolving threat.[68] Some of the challenges identified by this article include variation of terminology used in varying legislations, particularly, the current wording of the Internet Based Sexual Abuse (IBSA) provision within the EU Directive. This was narrow in scope and did not adequately reflect the experiences of victims. Overall, it can be argued that the Directive offered a piecemeal approach. Also, other identified challenges are the high rates of victim-blaming, and additional requirements of national provisions. Some legislations require either proof of the harm caused to the victim or of the underlying motivation of the offender and these additional requirements place a heavy burden of proof on the victim and increase the risk of victim-blaming attitudes within the courtroom.[69] This demonstrates the requirement for victim-friendly, robust legislative and policy responses involving a combination of international and national legal measures, including the development of specific laws and the adaptation of existing laws to address this online harm.[70]

The Directive does not specifically address IBSA as a distinct category of gender-based violence.[71] Rather, it touches upon certain aspects by establishing minimum standards for criminalization and harmonizing measures related to prevention, victim assistance and support, and prosecution.[72] For adequate victim assistance and support, this paper also adds the importance of training law enforcement agents and legal professionals so they understand the dynamics of TFGBV and how to offer best response and support to victims. Investigative and prosecutorial responses must be strengthened.

Legal Frameworks in Developing Countries

Developing nations confront particular legal difficulties caused by insufficient funding, shoddy institutional frameworks, and a dearth of knowledge about cutting edge technologies.[73] Additionally, in many developing countries such as Nigeria, there is a lack of comprehensive strong data protection and AI technologies regulations. For a proactive regulatory approach, a comprehensive legal framework for AI technologies, is appropriate for governing the gathering, storing, and use of personal data provides.[74] Where this is

[67] Ibid
[68] Ibid
[69] Ibid

[70] The Global Partnership (n18)
[71] Carlotta Rigotti (n65)
[72] Ibid
[73] Patrick Chukwunonso Aloamaka and Moses Ogorugba Omozue, 'AI and Human Rights: Navigating Ethical and Legal Challenges in Developing Nations', (2024) 6 Khazanah Hukum 2
[74] Abdulhameed Salihu, 'Regulating the Future: The Current State and Prospects of Artificial Intelligence Policy in Nigeria,' 2025 Available at SSRN <https://ssrn.com/abstract=5117653 or http://dx.doi.org/10.2139/ssrn.5117653> assessed 30/04/2025

lacking, a significant gap is created, and this makes people in the country susceptible to abuse and privacy violations.[75] This then generates a legal reactive situation where the law has to react after the problem starts to exist.

In Indonesia, the legal framework for data protection and AI regulation is still in its infancy.[76] In South Africa, there is lack of transparency and accountability in AI systems which further complicates efforts to ensure fairness and uphold human rights, such as the right to non-discrimination and equal protection under the law.[77] There are concerns that underscore the urgent need for comprehensive data protection laws in Zimbabwe to safeguard citizens' rights.[78] In these developing nations, there are benefits and risks associated with the use of artificial intelligence but it appears the risks and harms victims suffer outweigh the benefits. Among others, some major benefits AI offers humans include providing platforms for outperforming medical specialists in diagnosing certain diseases, automated hiring systems and measures intended to improve security. By using AI generative tools in these sectors to improve our lives, where there are no clear-cut legal regulations and laws regarding the collection, storing of personal data, these AI tools have the potential to pose more threat to the society particularly in these developing countries.

These threats could be creating opportunities for online harms targeting already oppressed groups like vulnerable marginalised women and girls. Therefore, this paper argues that without adequate legal framework for AI globally which can be implemented in developing nations, the risks significantly outweigh the benefits. Therefore, the next section highlights some theoretical analysis explaining the urgency for a comprehensive global AI legal framework available for developing nations.

Some Theories Justifying the Inclusion of online Gender-Based Violence into International Law

Critical Information Theory: According to De Silva De Alwin, critical information theory (CIT) focuses on more structural remedies that address the root causes of violence through preventative mechanisms.[79] CIT engages culture and cultural change and so, this model would also consider how culture and information intersect and draw attention to the engagement of men as leaders and role models.[80] Therefore, efforts to address technology facilitated violence against women would include education on digital violence. ADDMORE

Social Justice Theory: Kant's social justice theory rooted in respect for human dignity explains that while AI offers opportunities for development, careful consideration must be given to ensure its benefits are distributed fairly and do not disproportionately harm marginalized communities. AI's development in developing countries raises concerns

[75] Ibid
[76] Patrick Chukwunonso Aloamaka (n73)
[77] Ibid
[78] Ibid
[79] Rangita de Silva De Alwis (n56)
[80] Ibid

about social justice particularly regarding potential exacerbation of inequalities. By embracing Kant's social justice theory, AI development in developing countries can be guided by principles of fairness, autonomy, and respect for human dignity.

Deontological Ethics: From a deontological ethics perspective, the use of AI must respect fundamental human rights and ethical principles, such as privacy, fairness, and autonomy. In developing nations, where resources and infrastructure may be limited, these principles are crucial for ensuring that AI technologies are used ethically and benefit all members of society, rather than intensifying existing inequalities, particularly among women and girls.

Criminal Law Intervention: Is International Criminal Law (ICL) ready to accommodate TFGBV against women?

Earlier in this paper, it has been established that new AI technologies have the potential to advance the perpetration of online gender based violence and other forms of crime. Also established here is the fact that technology can serve as the vehicle by which certain crimes are committed or lead to new offences. These could be gendered international online crimes targeting some who may not be able to access redress such as women and girls. These marginalised group could be young people, individuals from varied sexualities as LGBTQ+, Black and minoritised women, refugees, asylum seekers, deaf and disabled women and girls as well as those with communication or literacy barriers. Women and girls in humanitarian contexts and those who are not digitally connected may face challenges due to lack of relevant services and support.

This paper suggests that as AI and technology continue to advance, perpetrators of online gender based violence continue to devise new ways of using it against women and girls. As this crime advances, in some cases, it constitutes transnational risks that transcend national boundaries and jurisdictions.[81] Therefore, it is expected that international criminal law (ICL) should also continue to evolve to accommodate new types of harm within the ambit of online gender-based violence and other online harms.

Interestingly, the UN General Assembly adopted the cybercrime convention, on December 24, 2024.[82] Remarkably, this becomes the first international criminal justice treaty of the 21st Century informed by various stakeholders, including civil society, the academy, and the private sector.[83] Following this, UN Member states adopted the "Countering the use of information and communications technologies for criminal purposes," otherwise known as the Cyber Crime Convention.[84]

The Preamble to the Convention states,

---

[81] Dorothy Estrada Tanck, 'Cyberspace and Women's Human Rights in the International Legal Order: Transnational Risks and Gender-Based Violence' (2024) 16 Cuadernos Derecho Transnacional 192

[82] Jule Pattison-Gordon, *United Nations Approves Draft Global Cyber Crime Treaty*, GOV'T TECH. (Aug. 13, 2024), <https://www.govtech.com/security/united-nations-approves-draft-global-cyber-crime-treaty>

[83] Rangita de Silva De Alwis (n56)

[84] Julie Pattison-Gordon (n82)

> Recognizing the importance of mainstreaming a gender perspective in all relevant efforts to prevent and combat the offences covered by this Convention, in accordance with domestic law.[85]

On the contrary, this does not follow up with substantive provisions that could further strengthen the gender perspective of online crimes against women. This paper argues that although the treaty covers TFGBV as it affects the girl child, which is good progress, women on the other hand appear to be excluded. This exclusion may stem from the reluctance to recognize sexual violence and TFGBV as international crimes.

Article 14-16 of the Convention address offenses related to

"online child sexual abuse or child sexual exploitation material" and calls for establishing criminal offenses under criminal law:

(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system;

(b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system;

(c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;

(d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence

Remarkably, the ICC rendered a guilty verdict against Jean-Pierre Bemba, ex-president of the Democratic Republic of Congo, for his involvement in war crimes and crimes against humanity in the Central African Republic during a 2002–2004 operation.[86] This decision is the first by the ICC to address sexual violence as a weapon of war and in the context of command responsibility.[87] Notably, the ICC in Bembe's case substantiates international offences of sexual violence and increases the visibility of women as victims of international crimes. It is hopeful that this improvement paves the way for the recognition of online gendered violence impact on women by the Draft UN Treaty.

Notably, there are elements of crime currently existing in the international criminal law framework that share some similarities with elements of these new crimes committed online. Identifying these old and new crimes with similar elements could make it easier for international criminal law to accommodate the new crimes within its framework. Gendered crimes are already available under ICL, the online component that aggravates

[85] Ibid
[86] Marie-Alice D'Aoust, 'Sexual and Gender-based Violence in International Criminal Law: A Feminist Assessment of the Bemba Case', 2016 International Criminal Law Review 17
[87] Ibid

the harm can and should be considered as worsening the offence, such as in the gravity assessment or at sentencing.[88]

In the context of online harms, sexual violence is closely linked to personal dignity, as the physical harms that can result from the sexual violence are not typically present given the nature of the digital space.[89] Distributing footage of sexual assaults or sharing nude images without consent online or being made to watch such footage is an example of an online harm that existing international criminal law frameworks on sexual violence should be able to address.[90]

As exemplified by the Rome Statute, provisions criminalizing forms of sexual violence are often vague. [91] It can be argued that the lists of acts included under Articles 7(g) (crimes against humanity) and 8(2)(b)(xxii) and 8(2)(e)(vi) (war crimes) are, indeed, non-exhaustive and allow for room for interpretation.[92] The crime of sexual slavery already exists under the Rome Statute and in this instance, using the internet as a forum to purchase or sell persons could constitute the offence as a crime against humanity or a war crime should the other elements of the crimes be met.[93] Arguably, as a way of enhancing the effectiveness of the law, including gendered crimes with similar elements as crimes against humanity or war crimes (as appropriate) is expected to help reduce the existing vagueness within the above ICL provisions.

However, a key challenge which would likely emerge from the arguments above could be whether hate speech and disinformation on social media websites should constitute main element of the International Criminal Court Office of The Prosector's case.[94] This paper suggests that if the harm suffered can be linked to harm to personal dignity, then that could qualify the online harm as a crime under ICL. Additionally, the issue of jurisdiction is another challenge which could emerge should online hate speech and disinformation become a crime under ICL. Another challenge of jurisdiction could be where online hate speech is perpetrated from multiple states (some of which might not even be known, as users can be anonymous and hide their locations).[95] In this case, it would be difficult to determine a jurisdictional or legal basis for prosecution, therefore, further research and a multi-stakeholder approach is required to determine how issues of jurisdiction can be resolved. More research is also required to determine how best to include newer online gendered violence that cause harms under ICL and in turn, to deliver more justice for victims.

---

[88] Sarah Zarmsky, 'Is International Criminal Law Ready to Accommodate Online Harm? Challenges and Opportunities', (2024) 22 Journal of International Criminal Justice 1

[89] Ibid

[90] Ibid

[91] Ibid

[92] For instance, Art. 7(g) (crimes against humanity) includes 'any other form of sexual violence of comparable gravity' to the listed acts, and both provisions under Art. 8(2) (war crimes) include 'any other form of sexual violence also constituting a grave breach of the Geneva Conventions'. Art. 7(g), 8(2)(b)(xxii), and 8(2)(e)(vi) ICCSt

[93] Art. 7(1)(g)-2, Art. 8(2)(b)(xii)-2, and Art. 8(2)(e)(vi) (crimes against humanity)-2 Elements of Crimes

[94] Sarah Zarmsky (n88)

[95] Ibid

Understandably, new technologies, and newer online gender-based violence continue to develop. Similarly, online harms may become more and more different from those recognized by ICL, and the only solution might be to create an entirely new crime, which would be much more difficult in practice. More limitations are encountered in the newly formulated UN legislations on artificial intelligence. Most of these documents do not make direct reference to women and the specific issues women face in the digital age, given that women constitute a majority of those impacted by this pandemic.

Some Existing Gaps within UN Instruments on Artificial Intelligence

Here, this paper identifies the gap in the UN Secretary General's Global Digital Compact (GDC) referenced earlier in the introduction section of this work. This document fails to mention the Convention on the Elimination of Discrimination against Women (CEDAW) in addressing all forms of violence, including sexual and gender-based violence, facilitated or amplified by technology.[96] Also, for a more comprehensive and globally inclusive framework, the Preamble in the UN GA Resolution on AI does not specifically recognize the Convention on the Elimination of Discrimination against Women (CEDAW) and other human rights treaties. As a part of the broader GDC effort, the UN General Assembly on AI mainly focuses on the role of the UN in achieving global consensus on AI development.

In 2018, the UN Special Rapporteur on Violence Against Women, its Causes and Consequences ("UNSRVAW") recognized the diverse nature of online violence against women, including its sexualized forms.[97] Furthermore, Paragraph 6 of the CEDAW General Recommendation No. 35 (2017) on gender-based violence against women, updating general Recommendation No. 19 (1992) acknowledges that gender-based violence against women manifests itself on a continuum of multiple, interrelated, and recurring forms, in a range of settings, including technology-mediated settings.[98] Consequently, it is important that the GA Resolution recognizes online violence as a category of gender-based violence and would signify a challenge against achieving the SDGs.[99]

Additionally, the Draft Cyber Crime Convention calls upon States to "adopt appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat [cybercrime] more effectively at the national, regional and international levels. Arguably, this paper interprets this to mean that instead of this Treaty clearly adding substantive provisions that reflect how TFGBV impacts women and the prescribed ways for Member States to protect women globally, the Treaty leaves Member States with this discretion. This creates a lacuna for certain

[96] Rangita de Silva de Alwis (n27)

[97] United Nations Human Rights Council Special Procedures, 'Special Rapporteur on violence against women and girls', <https://digitallibrary.un.org/record/1641160?ln=en > assessed 19 May 2025

[98] *Comm. on the Elimination of All Forms of Discrimination Against Women*, General Recommendation No. 35 (2017) on Gender-Based Violence Against women, Updating General Recommendation No. 19 (1992), U.N. Doc. CEDAW/C/GC/35 (July 26, 2017)

[99] Rangita de Silva De Alwis (n27)

States to adopt the doctrine of reservation when interpreting their obligation to the Treaty.

Recommendations: possible solutions/way forward

The call for ICL to recognise and accommodate online GBV as it affects women is so there is a shared language and global infrastructure around which different stakeholders can engage.[100] The protection of human dignity, as argued by deGuzman, is a central reason for why acts are criminalized under ICL.[101] The global nature of the internet requires international cooperation to address online GBV. This includes sharing information, coordinating enforcement efforts, and developing common standards such as from ICL for addressing online abuse.

As such, a multi-stakeholder approach which requires collaboration between governments, technology companies, civil society organizations, and other stakeholders becomes relevant. This encompasses the formulation of standardised measures for tackling this online gendered crime, the development of policies and guidelines to address online abuse, the provision of support services for survivors, and efforts to raise awareness about the issue.

According to this paper, one of the ways a uniformed approach can be achieved is by the amendment of CEDAW's provisions and the newly formulated Draft Cybercrime Treaty. Being that both Conventions share similar scope and purpose, the newly formulated convention should be amended to specifically capture issues impacting women in the digital space. That way it builds upon the already existing CEDAW and Member States who are already familiar with CEDAW can domesticate and implement the new Treaty.

Notwithstanding, many countries have laws that address cybercrime, including online harassment and abuse. These existing laws, however, may not fully encompass the specific challenges and harm posed by online gender-based violence (GBV) and the use of AI to facilitate such violence and abuse. Therefore, there is a pressing need for the adaptation and extension of these cybercrime laws to effectively combat the nuances of AI-enabled online GBV. States need a uniformed approach from ICL which enables them to protect women from transnational digital authoritarianism. This is in sync with States' responsibility to protect those living within their jurisdictions and to push back against the draconian practices of dictatorships that are now extending far beyond their borders.

Further, to justify the inclusion of new harms into ICL, this paper suggests that a harms-based approach can be adopted. This allows for new interpretations of international crimes, in which novel harms are compared to harms traditionally encompassed by ICL to justify their inclusion. International criminal law should include provisions for newer forms of online abuse, such as deep fakes, AI-generated misinformation, and the non-

[100]Jason Pielemeier, "The Advantages and Limitations of Applying the International Human Rights Framework to Artificial Intelligence," Data & Society: Points, June 6, 2018, https://points.datasociety.net/the-advantages-and-limitations-of-applying-the-international-human-rights-framework-to-artificial-291a2dfe1d8a.

[101] Margaret M. deGuzman, *Shocking the Conscience of Humanity: Gravity and the Legitimacy of International Criminal Law* (OUP, 2020)

consensual distribution of intimate images. Additionally, there should be clear definitions and penalties for these offences to ensure that perpetrators are held accountable and that victims receive justice.

Further, it is also important to address the digital divide and ensure that all individuals (women and girls) have equal access to digital technologies and the internet, including those who may be vulnerable to online GBV. Efforts should be made to close the digital divide gap among women and girls particularly in developing nations.

Conclusion

Clearly, significant international, regional and national efforts have been made to combat online gender-based violence, however, more is yet to be done particularly to provide a standardised measure in tackling the crime and protecting women and girls. A standardised approach is critical being that geographic distance emboldens the pile-on effect in the online space. Multiple offenders from disparate locations in most circumstances join forces in harassing and bullying a single woman, shaping a culture of sexism and misogyny in the virtual world. Undoubtedly, this paper highlighted that technology facilitated gendered violence blurs the lines between the real and virtual worlds. In this digital space, online harassment and abuse targeted at women, girls and minorities spill into the real world causing both physical and psychological violence in direct and indirect forms. This online harm which is about power, control and power imbalance also constitute human rights abuses. Therefore, it becomes imperative for the Draft Cyber Crime Convention and the UN GA Resolution on AI to adequately recognise CEDAW and build on CEDAW's existing framework on gender-based discrimination affecting women. Inclusion of an intersectional feminist thought and critical information theory according to this paper, introduces a gendered recognition of the impact of these online crimes on women. These calculated efforts create room for a gender-based violence framework informed by critical information theory.