University of Pennsylvania Carey Law School
Penn Carey Law: Legal Scholarship Repository

Articles | Faculty Works

3-2024

A Rapidly Shifting Landscape : Why Digitized Violence is the Newest Category of Gender-Based Violence

Rangita de Silva de Alwis
University of Pennsylvania Carey Law School, rdesilva@law.upenn.edu

Follow this and additional works at: https://scholarship.law.upenn.edu/faculty_articles

Repository Citation
de Silva de Alwis, Rangita, "A Rapidly Shifting Landscape : Why Digitized Violence is the Newest Category of Gender-Based Violence" (2024). *Articles*. 320.
https://scholarship.law.upenn.edu/faculty_articles/320

This Article is brought to you for free and open access by the Faculty Works at Penn Carey Law: Legal Scholarship Repository. It has been accepted for inclusion in Articles by an authorized administrator of Penn Carey Law: Legal Scholarship Repository. For more information, please contact biddlerepos@law.upenn.edu.

15

A Rapidly Shifting Landscape : Why Digitized Violence is the Newest Category of Gender-Based Violence

Rangita DE SILVA DE ALWIS [1],

Faculty at the University of Pennsylvania Penn Carey Law School and the Wharton School of Business, Senior Fellow at the Harvard Law School Center on the Legal Profession

This paper proposes that new research on technology-facilitated violence must shape gender-based violence against women laws. Given the AI revolution, including large language models (" LLMs "), and generative artificial intelligence, new technologies continue to create power disparities that help facilitate gender-based violence both online and offline. The paper argues that the veil of anonymity provided by the digital realm facilitates violence ; and the automation capabilities offered by technology amplify the scope and impact of abusive behavior. Although the direct physical act of sexual violence is different from offline violence, there are similarities. Firstly, both acts share the structural gender and intersectional inequities that lie at the root of such conducts in the first place. Secondly, the defense that women and girls are free to exercise the option to leave an abusive online environment denies women's and girls' free exercise of rights to assembly and expression in the online public square. In the final analysis, although not all isolated acts of online violence meet a legal threshold, we need to see these acts as a part of a continuum of offline violence that call for new forms of discourse and a dynamic application of international women's human rights norms into evolving categories of violence.

Introduction

1 - Naming has the power to shift legal and social norms. Technology facilitated gender-based violence is still largely an unnamed crime. Technology facilitated misogyny has many faces, both figuratively and in real terms. FaceMash, the precursor to Facebook, was developed by Facebook creator Mark Zuckerberg in 2003, and was designed to compare women's physical looks in elite American colleges. The paper calls for the application of human rights theory, critical gender theory and critical information theory to address this type of technology facilitated gender-based violence. Critical Information Theory examines an asymmetry in power relations and unmasks the power inequalities behind structures. Critical information theory not only calls attention to biased data but also asks whether the structures for using information have a chilling effect on certain groups of users. Technology-facilitated violence has the effect of : 1) blurring the lines between the real and the virtual worlds where online harassment and abuse targeted at women and minorities spill into the real world, thereby causing both physical and psychological violence ; 2) digital and internet technologies are embedded in ubiquitous ways that compromise women's ability to seek freedom from violence and render abusers " omnipresent " ; 3) technology-facilitated gender-based violence, by its very nature, is both personal and structural.

The dichotomy between " online " and " offline " violence collapses when it is subject to scrutiny through the lenses of critical gender theory and critical information theory. This article proposes the revision of anti-violence against women frameworks to address the evolving category of coded violence. A new generation of laws on gender-based violence should focus not only on the punishment of the perpetrator but on more structural remedies addressing the root causes of violence through preventative mechanisms. Efforts to address technology facilitated violence against women would include education on digital violence, including critical information theory (" CIT "). Because CIT engages culture and cultural change, this model would also consider how culture and information intersect and draw attention to the engagement of men as leaders and role models.

Technology-driven violence has a shape-shifting quality. It has the effect of blurring the lines between the real and the virtual worlds of violence against women. Online harassment and abuse targeted at women and minorities spill into the real world, thereby causing both physical and psychological violence. Digital and Internet technologies are embedded in ubiquitous ways that compromise women's ability to seek freedom from violence and render abusers " omnipresent. " In this paper, I will critically explore the human rights framework, especially the Convention on the Elimination of Discrimination against Women (" CEDAW "), and the landscape of domestic laws and regulations which provide new normative frameworks for combating violence in the digital space. In the final analysis, I call for a new gender-based violence framework that is informed both by critical information theory and

1. Rangita de Silva de Alwis is faculty at the University of Pennsylvania Carey Law School and the Wharton School of Business. She is Hillary Rodham Clinton Distinguished Fellow on Global Gender Equity at the Georgetown Institute for Women, Peace and Security and Senior Fellow at the Harvard Law School Center on the Legal Profession where she was Visiting Faculty at the Harvard Kennedy School of Government. She will be a Visiting Fellow at Bonavero Institute for Human Rights, Oxford University in 2024. She was elected as an expert to the treaty body on the Convention on the Elimination of Discrimination against Women (CEDAW) for the 2023-2026 term. She thanks her colleague on the CEDAW Committee, Nicole Ameline, for her inspiration and for encouraging her to address new frontiers for the CEDAW. She also thanks her Research Assistant Yungjee Kim (Penn Carey Law " 25) and her student Octavie Jacquet, Editor in Chief of the Sciences Po Law Review for their leadership.

human rights to address technology enabled violence as a growing category of both interpersonal and structural violence.

Technology facilitated gender-based violence like other forms of gender-based violence is about power, control and power imbalance. You can see this in data bias, or algorithmic bias that occurs when predefined data types or data sources are intentionally or unintentionally treated differently than others. Data is not inherently neutral ; data control itself is a form of power. It has the potential for great good and for great harm. We need a new way of thinking about technology and data science –one that is informed by intersectional feminist thought.

1. THIS MOMENT IN TIME

2 - The emergence of brand-new technology, including large language models (" LLMs "), and generative artificial intelligence (" AI ") continues to create power disparities and help facilitate gender-based violence as an evolving category of violence. Writing recently, Noam Chomsky, one of the world's leading linguists, warns us : " machine learning...will degrade our science and debase our ethics by incorporating into our technology a fundamentally flawed conception of language and knowledge. " [2] To this, I would like to add that machine learning (" ML ") and other evolving technology can create a fundamentally flawed conception of not only language and knowledge, but of power, especially over those who have historically been rendered powerless.

While the #MeToo movement was a key inflection point that galvanized a new era of digital feminist activism, this moment of generative AI is sparking fresh concerns about synthetic media and deepfakes. Digital sexual violence is rapidly changing with the dizzying changes in AI. Newer-and more interactive-digital and online spaces such as deepfakes and generative AI offer hitherto unanticipated forms of gender-based violence. While these digital spaces replicate in some ways the gender inequality in human interactions which occur outside of online environments, these online spaces offer a dystopian forum that can amplify inequality and magnify violence against women. Technology has outpaced legal reform, and even our ability to envision new forms of online harms and digital violence in social media sites and online games.

A. - New Forms of Online Violence Against Women

3 - In the contemporary digital era, the Internet has emerged as a new battleground where violence against women manifests itself. Online gender-based violence (" OGBV ") harnesses digital technology to instigate threats, intimidation, and harassment, constituting a dynamic and ever-evolving phenomenon within the rapidly progressing realm of technology. OGBV encompasses various forms such as cyberstalking, online harassment, non-consensual dissemination of intimate images, doxing, slut-shaming, trolling, cyber-flashing, gendered hate speech, disinformation, misinformation, cyber smear campaigns, threats of sexual violence and murder, morphing, as well as the proliferation of AI-generated sexually explicit media.

The intersection of technology and violence highlights the dual nature of technological advancements. While technology offers unprecedented connectivity and accessibility, it also serves as a double-edged sword, providing a platform for perpetrating, targeting, harassing, and threatening women. In this increasingly interconnected world, technology has opened new avenues through which acts of violence against women can be perpetrated.

Firstly, a notable characteristic of OGBV is the ability for offenders to remain anonymous to their victims. This veil of anonymity provided by the digital realm not only enables their actions but also emboldens them in their abusive behavior. Secondly, the geographical distance facilitated by online platforms allows offenders to engage in abusive conduct from afar, without the need for physical proximity or even being in the same country as their victims. This geographical detachment provides a sense of detachment and impunity for the offenders. Thirdly, the automation capabilities offered by technology amplify the scope and impact of abusive behavior. Offenders can exploit technological tools to perpetrate their abuse more efficiently and with minimal effort. Moreover, the pile-on effect is a significant concern in the online space, where multiple offenders can join forces in harassing and bullying a sole individual. The digital platforms themselves, designed for easy and rapid dissemination of content, facilitate this collective harassment.

Most of all, the unequal power dynamics between men and women, along with the devaluation of women in society, permeate into the online sphere as an extension of offline belief systems. 85% of women reported encountering some form of OGBV. [3] Furthermore, 23% of women reported encountering online harassment at least once in their lives, and one in ten women experienced OGBV since the age of fifteen. [4] The impact of OGBV is substantial-for example, 20% of surveyed women journalists report withdrawing from all online interaction because of OGBV. [5]

The U.N. General Assembly recognized the growing concern of ICT-facilitated abuses against women human rights defenders, and the need for effective responses in line with human rights principles. [6]

The structure of the Internet and social media platforms creates echo chambers, where individuals reinforce their existing views through repetition and interaction within a self-contained bubble. This echo chamber phenomenon, devoid of opposing perspectives, leads to confirmation bias and has far-reaching social, political, and cultural effects. In the context of OGBV, an example of this phenomenon is the incel movement, an internet subculture that frequently expresses deeply misogynistic content. However, it is important to acknowledge that while technology can contribute to discriminatory behaviors, it also has the potential to promote gender equality and challenge societal norms and ideologies that perpetuate such abuses.

Several technological solutions have emerged to counter OGBV, such as smartphone applications and software that protect against stalkerware, malware, spyware, and trackers, as well as alert emergency contacts and services with geolocation features and crisis alarms. Additionally, there is a concerning trend of AI-powered chatbots, created as on-demand romantic or sexual partners, being subjected to abuse by users. This form of chatbot mistreatment often exhibits a gendered component, with men creating digital partners representing women and subjecting them to abusive language and aggression. Online forums on platforms like Reddit and Discord even provide spaces for abusers to share tactics and strategies for further harming their virtual partners.

2. Noam Chomsky et al., *The False Promise of ChatGPT*, NY Times (Mar. 8, 2023), https ://www.nytimes.com/2023/03/08/opinion/noam-chomsky-chatgpt-ai.html.

3. *Measuring the Prevalence of Online Violence Against Women*, The Economist : Intelligence Unit, https ://onlineviolencewomen.eiu.com/.

4. *Amnesty Reveals Alarming Impact of Online Abuse Against Women*, Amnesty Int'l (Nov. 20, 2017), https ://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.

5. Julie Posetti et al., *Online Violence Against Women Journalists : A Global Snapshot of Incidence and Impacts*, U.N. Educ., Sci. & Cultural Org. [UNESCO] (2020), https://www.icfj.org/sites/default/files/2020-12/UNESCO%20Online%20Violence%20Against%20Women%20Journalists%20-%20A%20Global%20Snapshot%20Dec9pm.pdf.

6. G.A. Res. 68/181, U.N. Doc. A/RES/68/181 (Jan. 30, 2014) (stating that " [ICT]-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights. ").

B. - Why Technology Facilitated Violence is Gender-Based Violence

4 - Although the direct physical act of sexual violence, and the degree of violation of sexual autonomy that arises from it, differ between online and offline worlds, both acts share the structural causes that lie at the root of such conduct in the first place : patriarchy, and historical power differences between the genders.

First, this power difference is inherent to the argument that women and girls are free to exercise the option to leave an abusive online environment which helps to take away women's and girls' right to equality, including their equal rights to the Internet and the online community. Secondly, online violence may result in direct physical, emotional and psychological violence-whether it be mental harm suffered as a result of online violence or bodily harm suffered offline.

Digital gender-based violence has many faces, both figuratively and in real terms. FaceMash, the precursor to Facebook, was developed by Facebook creator Mark Zuckerberg in 2003, and was designed to compare women's physical looks in elite American colleges. [7] More recently, feminist gaming critic Anita Sarkeesian was forced to leave her San Francisco home due to ongoing threats by online trolls had threatened to kill her parents, drink her blood, and rape her-all while publishing her personal details online. [8] Most horrifyingly, an interactive game was created in her likeness, in which players were encouraged to " beat up Anita Sarkeesian " by virtually punching an image of her face. [9]

These online threats against women in public life are common and have sometimes resulted in women leaving office. For instance, Diane Abbott, the first black member of Parliament in the U.K., was targeted with more than 8,000 tweets in the first six months of 2017 alone. [10] Maria Ressa, the Nobelist, has been subject to abuse for her stand against civil rights violations by the Duterte regime. Researchers analyzed nearly 400,000 tweets and more than 57,000 Facebook posts and comments directed at Ressa between 2016 and 2021 : while 60% of the online violence questioned Ressa's credibility as a journalist, 40% of the attacks were threats to physical safety including threats of rape and murder. [11] In the U.K., following years of online abuse over her political coverage, journalist Laura Kuenssberg announced that she would move to a new role at BBC. [12] Due to the harassment she has been a target of, she was assigned a bodyguard. [13]

C. - A Continuum of Violence : Deepfakes

5 - The proliferation of deepfakes, AI-generated images, videos, and other media content against women is another emerging category of violence that must be named in new and revised gender-based violence laws and by the CEDAW. Deepfake technology uses AI and facial mapping technology to merge, combine, and superimpose images and video clips onto one another to generate authentic-looking media called " deepfakes. " Pornographic deepfakes reinforce a culture that commodifies and objectifies women's bodies.

Companies such as DeepSwap.Ai allow an individual to upload an image or video and swap it with any number of faces a user chooses to upload. [14] Some websites explicitly promise to turn any person into a " porn star " by uploading their photo onto the website, which uses deepfake technology to swap the person's face into an adult. [15]

Deepfakes have become the new sites for violence against women and technology-facilitated abuse. Estimates suggest that more than ninety-five percent of deepfake videos on the Internet in 2019 were pornographic. [16] Companies like Google allow users to request the removal of involuntary fake pornography. [17] Facebook has expressed that they will address deepfakes and other manipulated media, including investigating AI-generated content and deceptive behaviors, in partnership with academic, government, and industry professionals to remove misleading images and punish perpetrators of media misuse. [18] DeepSwap.Ai's terms of service explicitly disallow the creation of pornographic deepfakes :

> [Y]ou shall not upload, share or otherwise transmit to or via the Services any content that : is...obscene, abusive, racially or ethnically offensive, pornographic, indecent, lewd, harassing, threatening, invasive of personal privacy.... [19]

D. - The Nexus Between Online Gender-Based Harassment and the Erosion of the Democratic Space

6 - In August 2020, Speaker Nancy Pelosi and other American women lawmakers, along with legislators around the world, wrote a letter to Facebook calling upon the platform to take action to protect female political actors from online attacks. The letter went on to say : " Make no mistake... [t]hese tactics, which are used on your platform for malicious intent, are meant to silence women, and ultimately undermine our democracies. " [20] Further, it read : " We are imploring Facebook to do more to protect the ability of women to engage in democratic discourse and to foster a safe and empowering space for women. " The letter was written in the aftermath of Facebook's refusal to take down a deep-fake video of her that was manipulated so she appeared intoxicated. [21]

The disproportionate and often strategic targeting of women politicians has both direct and indirect impact on the democratic process by driving women out of political office and muffling those who remain online. [22] While censoring free speech erodes the democratic space, a vibrant democracy calls for the full and equal

7. Katherine A. Kaplan, *Facemash Creator Survives Ad Board*, Harvard Crimson (Nov. 19, 2003), https ://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.
8. Soraya Nadia McDonald, *Gaming Vlogger Anita Sarkeesian is Forced from Home After Receiving Harrowing Death Threats*, Wash. Post (Aug. 29, 2014, at 5 :23 a.m. EDT), https ://www.washingtonpost.com/news/morning-mix/wp/2014/08/29/gaming-vlogger-anita-sarkeesian-is-forced-from-home-after-receiving-harrowing-death-threats/.
9. *Id.*
10. Anastasia Powell et al., *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan eds. Nov. 2022).
11. David Mass, *New Research Details Ferocity of Online Violence Against Maria Ressa*, Int'l Journalists " Network (Mar. 8, 2021), https ://ijnet.org/en/story/new-research-details-ferocity-online-violence-against-maria-ressa.
12. *Laura Kuenssberg to Step Down as BBC's Political Editor*, BBC (Dec. 20, 2021), https ://www.bbc.com/news/entertainment-arts-58996925.
13. Patrick Kingsley, *Why the BBC's Star Political Reporter Now Needs a Bodyguard*, NY Times (Sept. 27, 2017), https ://www.nytimes.com/2017/09/27/world/europe/uk-bbc-laura-kuenssberg-labour.html.
14. DeepSwap, https ://www.deepswap.ai/landing/playable-faces.
15. Kweilin T. Lucas, *Deepfakes and Domestic Violence : Perpetrating Intimate Partner Abuse Using Video Technology*, 17 Victims & Offenders 647 (2022).
16. Meredith Somers, *Deepfakes, Explained*, MIT Sloan (July 21, 2020), https ://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained.
17. *Remove Involuntary Fake Pornography from Google*, https ://support.google-.com/websearch/answer/9116649 ?hl=en.
18. Monika Bickert, *Enforcing Against Manipulated Media*, Meta Newsroom (Jan. 6, 2020), https ://about.fb.com/news/2020/01/enforcing-against-manipulated-media/.
19. However, in the U.S., online platforms are protected by Section 230 of the Communications Decency Act from civil liability for user-generated content.
20. Emma Goldberg, *Fake Nudes and Real Threats : How Online Abuse Holds Back Women in Politics*, NY Times (June 7, 2021), https ://www.nytimes.com/2021/06/03/us/disinformation-online-attacks-female-politicians.html.
21. Abram Brown, *Facebook Can Be Toxic for Female Politicians, Company Documents Show*, Forbes (Oct. 27, 2021, 04 :27pm), https ://www.forbes.com/sites/abrambrown/2021/10/27/facebook-can-be-toxic-for-female-politicians-company-documents-show/ ?sh=258e3f175020.
22. *See further*, Lucina di Meco & Saskia Brechenmacher, *Tackling Online Abuse and Disinformation Targeting Women in Politics*, Carnegie Endowment for Int'l Peace (Nov. 30, 2020), https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331 (detailing online gender-based abuse of female politicians around the world) ; Nina Jankowicz et al., *Malign Creativity : How Gender, Sex, and Lies are Weaponized Against Women Online*, Wilson Ctr. Sci. & Tech. Innovation Program (Jan. 2021), https://www.wilsoncenter.org/sites/default/files/media/uploads/documents/Report%20Malign%20Creativity%20How%20Gender

participation of both men and women online and offline. Female politicians are not only targeted disproportionately but also subjected to different forms of harassment and abuse based on physical appearance and sexuality. [23] All this has the very real potential to pose a chilling effect on the participation and engagement of women in civic and political life-not just as politicians but as participants in the online debates that now drive so much of political culture.

In October 2023, a former student from the National Polytechnic Institute, Mexico was charged in connection with a first-of-its-kind cases involving AI-driven digital violence. [24] The student had used AI to generate non-consensual deepfake pornography, digitally undressing fellow students, and subsequently profited from selling these manipulated images on the Internet. [25] The accused is currently facing charges related to privacy offenses, as outlined by the Olympia Law. [26] This legislation, specific to Mexico City, safeguards individuals from the creation and dissemination of intimate images without their consent. [27] Remarkably, this law appears to have anticipated the potential misuse of AI in such instances, reflecting the proactive nature of its provisions. [28]

In September 2023, the UK adopted the Online Safety Act-one of the most wide-ranging efforts by a Western democracy to oversee digital discourse. [29] These far-reaching guidelines have sparked discussions on the fine balance between free expression and prevention of harmful online content, with a specific focus on safeguarding children. [30] The bill defines " primary priority content that is harmful to children " as " content which encourages, promotes or provides instructions " [31] for " suicide, " [32] " an act of deliberate self-injury, " [33] and " an eating disorder. " [34] On the other hand, in 2020, the French Constitutional Council struck down similar regulations due to concerns about overreach and censorship. [35]

2. HUMAN RIGHTS FRAMEWORK

A. - International Human Rights Law's Response to Digital Violence

7 - The proliferation of digital violence is raising key normative and institutional challenges to the existing international human rights law and international women's human rights frameworks. A changing normative landscape creates new opportunities for promoting human rights in the digital age. We need a radical reinterpretation of existing human rights in order to allow them to meet the new conditions of the digital age.

International human rights law has always responded to the ways in which individuals and societies confront changing economic, social, and cultural conditions. It could be argued that the current " digital revolution " represents yet another moment for transformation in the international human rights law framework. This revolution also invites a process of normative transformation involving the articulation of new legally binding or soft law instruments. The UN Human Rights Council (" HRC ") has adopted a plethora of non-binding resolutions that advocate the extension of offline human rights to activities and interactions online. [36]

The EU Commission, too, is dealing in this moment with new regulations and those yet in the pipeline. [37] The Commission has promulgated a Declaration on Digital Rights and Principles for the Digital Age which addresses rights of individuals both offline and online. [38]

These evolving norms will be discussed under three pillars :

1° Due Diligence Principle

8 - The first involves efforts to strengthen corporate responsibility through the Business and Human Rights platform following the adoption of the Ruggie Principles, or the Guiding Principles on Business and Human Rights, a legally binding instrument on business and human rights. The Guiding Principles require businesses to exercise " human rights due diligence, " to impose legal liability for human rights abuses, to see to it that remedies are provided to victims, and to engage in international cooperation in the implementation of the instrument. This framework also applies to technology companies whose activities affect the enjoyment of digital human rights, and, in particular, to those operating online platforms, providing Internet services and developing AI products.

2° Extraterritoriality

9 - The second involves the extraterritorial reach of the human rights obligations of technology exporting countries in relation to the conduct of private companies. Although States are largely defined by territorial sovereignty and territorial jurisdiction, the evolving digital rights call for addressing the extra-territorial activity of non-state actors. [39] One transformation is the extra-territorial application of human rights obligations on governments to actively regulate private businesses.

The extra-territorial application of international human rights is manifest in the work of treaty bodies. For example, in 2018, the HRC Committee developed a jurisdictional standard covering conduct with extraterritorial effects that has " direct and reasonably foreseeable impact " on the enjoyment of the right to life. [40] In 2021, the Committee on the Rights of the Child (" CRC ") embraced " reasonable foreseeability " of impact as the test for exercising extra-territorial jurisdiction in a climate change case. [41]

In its 2014 review of the fourth periodic report of the US, the HRC Committee raised concerns about media reports describing surveillance activities undertaken by US security agencies both inside and outside US territory. These episodes included the collection of bulk data and metadata, and the alleged wiretapping of European leaders. The Committee recommended that the U.S. take the necessary measures to ensure that " any interference with the

%2C%20Sex%2C%20and%20Lies%20are%20Weaponized%20Against%20Women%20Online_0.pdf (same).

23. *Id.*
24. María Alejandra Trujillo, *Mexico : Arrest in Landmark AI-Related Digital Violence Case*, BNN (Nov. 26, 12 :29 PM), https ://bnn.network/breaking-news/crime/mexico-arrest-in-landmark-ai-related-digital-violence-case/.
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. Adam Satariano, *Britain Passes Sweeping New Online Safety Law*, NY Times (Sept. 19, 2023), https ://www.nytimes.com/2023/09/19/technology/britain-online-safety-law.html.
30. *Id.*
31. Online Safety Act 2023, 2023 ch. 50 § 61 (U.K.).
32. *Id.* at § 61(3).
33. *Id.* at § 61(4).
34. *Id.* at § 61(5).
35. *Freedom on the Net 2020*, Freedom House (last visited Nov. 26, 2020), https ://freedomhouse.org/country/france/freedom-net/2020.
36. *See e.g.*, G.A. Res. 68/167, [para] 3 (Dec. 18, 2013) ; G.A. Res. 69/166, [para] 3 (Dec. 18, 2014) ; G.A. Res. 73/179, [para] 3 (Dec. 17, 2018) ; G.A. Res. 75/176, [para] 3 (Dec. 16, 2020) ; Human Rights Council [HRC] Res. 26/13, U.N. Doc. A/HRC/RES/26/13, at 2 [para] 1 (June 26, 2014) ; HRC Res. 32/13, U.N. Doc. A/HRC/RES/32/13, at 3 [para] 1 (July 1, 2016) ; HRC Res. 38/7, U.N. Doc/HRC/RES/38/7, at 3 [para] 1 (July 5, 2018).
37. The EU AI Act was passed in December 2023 during the writing of this article. The European Commission president Ursula Von der Leyen heralded the AI Act as a " unique legal ; framework for the safety and fundamental rights of people and businesses. ". *See* Morgan Meaker, *The EU Just Passed Sweeping New Rules to Regulate AI*, Wired (Dec. 8, 2023 at 06 :20 PM), https ://www.wired-.com/story/eu-ai-act/.
38. European Declaration on Digital Rights and Principles for the Digital Decade, Commission Decl. at Ch. 1, COM (2022) 28 final (Jan. 26, 2022).
39. *See e.g.*, Mariarosaria Taddeo & Luciano Floridi, *New Civic Responsibilities for Online Service Providers*, *in* the responsibilities of online providers 1 (Mariarosaria Taddeo & Luciano Floridi eds., 2017).
40. Human Rights Committee [HRC Committee], General Comment No. 36 : The Right to Life, [para][para] 22, 63 U.N. Doc. CCPR/C/GC/36 (2018).
41. *Sacchi v. Argentina*, Views of the C.R.C., [para] 10.7, U.N. Doc. CRC/C/88/D/104/2019 (2021).

right to privacy complies with the principles of legality, proportionality, and necessity, regardless of the nationality or *location* of the individual whose communications are under *direct* surveillance. " [42]

3° Interrelatedness of Human Rights Norms

10 - The third pillar is the emerging effort in relation to a holistic understanding of the core treaties. This involves giving effect to the 1993 Vienna Declaration core values concerning the indivisibility, interdependence, and interrelatedness of all human rights, as well as the drawing of treaty bodies from each other's jurisprudence. [43]

The international human rights agenda itself provides a powerful framework to prevent coded violence against women, including the CEDAW, and the Declaration on the Elimination of Violence against Women. The CEDAW General Recommendation 35 Paragraph 6 acknowledges that :

> Gender-based violence against women, whether committed by States, intergovernmental organizations, or non-State actors, including private persons... It manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings...

Furthermore, the Declaration on the Elimination of Violence Against Women's recognition that " violence against women is a manifestation of historically unequal power relations between men and women, which have led to domination over and discrimination against women by men and to the prevention of the full advancement of women " provides us with a strong conceptual framework for the understanding of coded bias.

In 2018, the U.N. Special Rapporteur on Violence Against Women, its Causes and Consequences (" UNSRVAW ") recognized the diverse nature of online violence against women, including its sexualized forms :

> Online and ICT-facilitated acts of gender-based violence against women and girls include threats of such acts that result, or are likely to result, in psychological, physical, sexual or economic harm or suffering to women. (...) ICT may be used directly as a tool for making digital threats and inciting gender-based violence, including threats of physical and/or sexual violence, rape, killing, unwanted and harassing online communications, or even the encouragement of others to harm women physically.

Addressing online violence against women for the first time in an official UN report, Dubravka Šimonovic, the then-UN Special Rapporteur, presented her report to the HRC and argued that " online and ICT-facilitated forms of violence against women have become increasingly common, particularly with the use, every day and everywhere, of social media platforms and other technical applications. " [44] The Special Rapporteur called for " due diligence " on the part of businesses to eliminate online violence against women and address the phenomenon of violence against women facilitated by new technologies and digital spaces from a human rights perspective. She posited the interrelated rights to live a life free from violence to freedom of expression, to privacy, to have access to information shared through information and communications technology (" ICT "), and other rights.

Addressing the widespread and systemic structural discrimination and gender-based violence against women and girls, facilitated by new types of gender-based violence and gender inequality in access to technologies, which hinder women's and girls " full enjoyment of their human rights and their ability to achieve gender equality, she acknowledged that the vernacular in this area is still developing and not univocal. The Special Rapporteur referred to " online violence against women " as a more user-friendly expression but also used the terms " cyberviolence " and " technology-facilitated violence. " While the report argued the principle that human rights protected offline should also be protected online, it is now obvious that offline bleeds into online and vice versa.

Given the significant role played by technology companies in facilitating the enjoyment of digital human rights, including online free speech, online privacy, and the right to be forgotten, it is hardly surprising that human rights officials, such as the UN Special Rapporteurs for Freedom of Expression and Privacy, have turned their attention increasingly towards the regulatory role of governments vis-à-vis technology companies. [45]

The HRC Committee has had the opportunity to review the matter of export of digital products manufactured by private companies in its review of Italy in 2017. The Committee expressed concern about :

" Allegations that companies based in the State party have been providing online surveillance equipment to Governments with a record of serious human rights violations and about the absence of legal safeguards or oversight mechanisms regarding the export of such equipment. " [46]

It recommended that " measures are taken to ensure that all corporations under its jurisdiction, in particular technology corporations, respect human rights standards when engaging in operations abroad. " The matter of export controls relating to surveillance technology has also been taken up by the UN Special Rapporteur on Freedom of Expression, who has reported on the harmful effects on political expression of resort by governments to spyware programs and called for a moratorium on the export of such technology. [47]

The HRC has examined digital forms of violence and reaffirmed that the violence against women in digital contexts is a growing concern and emphasized the need to address systemic gender-based discrimination through effective responses in accordance with human rights. [48] Resolution 38/5 underscored the multi-jurisdictional and transnational nature of violence against women and girls in digital contexts, calling for active cooperation among different actors (States and their law enforcement and judicial authorities, and private actors) to detect, report, and investigate such crimes. [49] It also highlighted the critical role that digital technology companies, especially Internet service providers and digital platforms, have in ameliorating the damage caused by digital violence. [50]

In 2012, the HRC declared that " the same rights that people have offline must also be protected online, " [51] and in 2015, recognized that domestic violence could include acts such as cyberbullying and cyberstalking. [52] The UN General Assembly acknowledged,

42. HRC Committee, Concluding Observations in the Fourth Periodic Report of the U.S.A., [para] 22, U.N. Doc, CCPR/C/USA/CO/4 (2014) (emphasis added). The extra-territorial use of drones was another topic discussed in the same US periodic review session.
43. Vienna Declaration and Programme of Action, U.N. Doc. A/CONF.157/23 (July 12, 1993).
44. Dubravka Šimonovic (Special Rapporteur on Violence Against Women, Its Causes and Consequences), Rep. on Online Violence Against Women and Girls From a Human Rights Perspective, U.N. Doc. A/HRC/38/47 (June 18, 2018).
45. *See e.g.*, Irene Khan (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 18 [para] [para] 90-91, U.N. Doc. A/HRC/47/25 (Apr. 13, 2021) ; David Kaye (Special Rapporteur on the Freedom of Opinion and Expression), *Rep.*, at 22 [para] 57, U.N. Doc. A/74/486 (Oct. 9, 2019).
46. Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Italy, 36, U.N. Doc. CCPR/C/ITA/CO/6 (2017).
47. *See e.g.*, Special Rapporteur on the Freedom of Opinion and Expression, *Rep.*, at 14-15, 48-49, U.N. Doc. A/HRC/41/35 (May 28, 2019).
48. HRC Res. 38/5, U.N. Doc. A/HRC/RES/38/5 (July 4, 2018).
49. *Id.* at [para] 11.
50. Id. at [para] 10(d). (calling for States to " strengthen or adopt positive measures, including internal policies, to promote gender equality in the design, implementation and use of digital technologies with a view to eliminating violence against women and girls, and to refrain from presenting women and girls as inferior beings and exploiting them as sexual objects.... ").
51. HRC Res. 20/8, U.N. Doc. A/HRC/RES/20/8, at [para] 1 (July 5, 2012).
52. HRC Res. 29/14, U.N. Doc. A/HRC/RES/29/14, at [para] 4 (July 22, 2015).

just a year later, that women were particularly affected by violations of the right to privacy in the digital age and called upon all States to further develop preventive measures and remedies. [53] The HRC reaffirmed this call again in 2017, noting that abuses of the right to privacy in the digital age may affect all individuals, with particular effects on women, children and marginalized groups. [54]

B. - Mining the CEDAW and Regional Treaties

11 - As the only universal and widely ratified bill of rights for women, the Convention on the Elimination of Discrimination against Women (" CEDAW ") is the most authoritative treaty to combat technologically facilitated violence against women. General Recommendation No. 35, which builds on CEDAW General Recommendations No. 19, can be a tool to combat pornographic deepfakes internationally. General Recommendation No. 35 refers specifically to digital forms of gender-based violence and provides a comprehensive list of measures for State parties to support prevention, protection, prosecution, punishment, and reparations of digital gender-based violence, points that could easily translate to a national strategy to combat deepfakes. [55] For prevention, the Committee recommended that State parties " adopt and implement effective legislation and other appropriate measures to address the underlying cause of gender-based violence. " [56] General Recommendation No. 35 represents preliminary steps by the CEDAW Committee to address digital gender-based violence and frequently neglected negative consequences arising from technological advancements. [57] This sentiment raises a broader inquiry if there should be a new CEDAW Committee general recommendation that addresses AI-driven gender-based violence, which has been largely under-analyzed through the lens of women's rights.

Furthermore, the Declaration on the Elimination of Violence Against Women's recognition " that violence against women is a manifestation of historically unequal power relations between men and women, which have led to domination over and discrimination against women by men and to the prevention of the full advancement of women " provides us with a strong conceptual framework for the understanding of algorithmic bias.

Regional treaties on women's rights such as the Maputo Protocol [58] and the Belem Do Para treaty [59] are silent on technology facilitated violence against women. However, the Secretariat of the Violence Against Women Division of the Council of Europe, published a paper titled " Protecting women and girls from violence in the digital age – The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women. " The Budapest Convention addresses directly and indirectly some types of cyberviolence against women. [60]

C. - Domestic Frameworks

1° Korean Legal System Reform

12 - In response to the Nth Room case which ripped apart the veiled world of online violence [61], the Korean National Assembly has enacted a series of amendments to various legislative acts, including the Criminal Act, Act on Special Cases Concerning the Punishment of Sexual Crimes, Act on Regulation and Punishment of Criminal Proceeds Concealment, Act on the Protection of Children and Youth Against Sex Offenses, Act on Promotion of Information and Communications Network Utilization and Information Protection, and the Telecommunications Business Act. [62]

One key amendment to the Criminal Act involves Article 305, which now stipulates that individuals aged nineteen or older who engage in sexual intercourse or indecent acts with individuals aged thirteen or older but under sixteen shall be subject to punishment. [63] This amendment raises the age at which consent can be given for statutory rape from thirteen to sixteen years, thereby enhancing the protection of minors. [64]

Another significant amendment to the Criminal Act introduces a new provision making individuals who prepare or conspire with the intent to commit rape, [65] imitative rape, [66] or quasi-rape [67] are liable to imprisonment with labor for a maximum period of three years.

However, concerns have been raised regarding the adequacy of punishments in cases like the Nth Room, where the primary evidence consisted of self-taken images and footage shared in chatrooms. These concerns stem from the difficulty in establishing conclusive proof that the violence and threats inflicted on over seventy victims through chat messages resulted in the actual crimes

53. G.A. Res. 71/199, U.N. Doc. A/RES/71/199, at [para] 5(g) (Dec. 19, 2016).
54. HRC Res. 34/7, U.N. Doc. A/HRC/RES/34/7 (Apr. 7, 2017).
55. CEDAW, 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). (" Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private... and the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments. ")
56. *Id.*
57. *Id.* (" Gender-based violence against women, whether committed by States, intergovernmental organizations, or non-State actors, including private persons... It manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings... ").
58. Protocol to the African Charter on Human and Peoples " Rights on the Rights of Women in Africa, better known as the Maputo Protocol, is an international human rights instrument established by the African Union.
59. Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women, better known as the Belém do Pará Convention.
60. In fact, in March 2019, the Committee of Ministers of the Council of Europe adopted a new recommendation on preventing and combating sexism that contains a seminal definition of sexism, including online and via new technologies, Sexism is defined as : " Any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of : I. violating the inherent dignity or rights of a person or a group of persons ; or II. resulting in physical, sexual, psychological or socio-economic harm or suffering to a person or a group of persons ; or III. creating an intimidating, hostile, degrading, humiliating or offensive environment ; or IV. constituting a barrier to the autonomy and full realisation of human rights by a person or a group of persons ; or V. maintaining and reinforcing gender stereotypes. "
61. The Nth Room case (2020) involved an infamous network of chatrooms in the Telegram messaging app, women and girls in South Korea were blackmailed and coerced into sharing non-consensual images of sexual acts. The police identified approximately 1,100 women and girls who were victims of this network. The two most infamous of these chatrooms were the Nth Room (which refers to any one of eight different chat rooms) and the Doctor's Room. In both rooms, women and girls-some of them middle-school age-were deceived and coerced into uploading sexually explicit photos and videos of themselves to Telegram, which were then sold and shared in chatrooms with up to tens of thousands of users. The victims were often ordered to film themselves performing lewd acts under the threat that noncompliance would result in the release of the content to their families and-in the case of minors-their educational institutions.
62. Wonchul Kim, *'Nth Room Prevention Law " Passed : Imprisonment For Up to 3 Years For Possessing or Viewing Sexual Exploitation Media*, Hankyoreh (Apr. 29, 2020), https ://www.hani.co.kr/arti/politics/assembly/942627.html.
63. Hyeongsabeob [Criminal Act] art. 305(2), partially amended by Act. No. 17572, Dec. 8, 2020 (S.Kor.).
64. *Id.*
65. *Id.* at art. 297. (" [A] person who, by means of violence or intimidation, has sexual intercourse with another shall be punished by imprisonment with labor for a limited term of at least three years. ").
66. *Id.* at art. 297-2. (" A person who, by means of violence or intimidation, inserts his or her sexual organ into another's bodily part (excluding a genital organ), such as mouth or anus, or inserts his or her finger or other bodily part (excluding a genital organ) or any instrument into another's genital organ or anus shall be punished by imprisonment with labor for a limited term of at least two years. ").
67. *Id.* at art. 299. (" A person who has sexual intercourse with another or commits an indecent act on another by taking advantage of the other's condition of unconsciousness or inability to resist shall be punished in accordance with [rape, imitative rape, and indecent act by compulsion]. ").

listed in the provision. [68] Therefore, it is necessary to carefully examine the evidence and ascertain whether the existing legal framework adequately addresses the offenses committed in cases like the Nth Room, particularly with regards to the connection between the violence inflicted and the specific crimes specified in the aforementioned provision.

In response to the imperative of preventing crimes resembling the Nth Room case, the Act on Special Cases Concerning the Punishment of Sexual Crimes also underwent notable reform. These amendments introduced significant changes to the penalties associated with various offenses, including special rape, [69] aggravated rape, indecent act by compulsion against minors under the age of thirteen, and indecent acts in crowded places. [70]

One salient modification pertains to special rape, for which the penalty has been enhanced to imprisonment with labor for an indefinite term or for a minimum of seven years, in contrast to the previous minimum of five years. [71] Similarly, the penalty for aggravated rape has been raised from five to seven years. [72], [73] In the case of indecent act by compulsion against minors below the age of thirteen, the relevant provision has been revised to eliminate the previous fine range of thirty to fifty million won (30,000 to 50,000 USD), replacing it with a penalty of imprisonment with labor for a minimum term of five years. [74], [75] Regarding indecent acts in public settings, the amendment remains unchanged (not exceeding three million won) but the amendment now allows for imprisonment of up to three years as an alternative, compared to the former maximum sentence of one year. [76], [77]

Furthermore, an amendment of particular significance concerns Article 13, which addresses obscene acts through communication media. [78] The revised provision encompasses the transmission of any words, sounds, writings, pictures, images, or other materials that may induce a sense of sexual shame or aversion, with the intent to arouse or satisfy the sender's or recipient's sexual urges. Violators are now subject to imprisonment with labor for a maximum of two years or a fine not exceeding twenty million won (20,000 USD). [79] This represents a departure from the previous arrangement, where the same act warranted a comparable period of confinement but entailed a maximum fine of five million won (5,000 USD). [80]

While substantial and noteworthy amendments have been made to provisions concerning the production and dissemination of sexually exploitative media, it is important to note that the language of the Act still lacks the nuanced recognition that the victims are, indeed, victims of exploitation. Although the penalties have been augmented for the filming and distribution of sexually exploitative photographs and videos taken without the subject's consent, the description of such materials as capable of causing " sexual stimulus or shame " fails to acknowledge the exploitative nature of these images. [81] In contrast, the Children and Youth Sex Offense Protection Act explicitly designates victimizing videos as sexually exploitative material, thereby recognizing the victims as victims of exploitative crimes. [82] The Act on Special Cases Concerning the Punishment of Sexual Crimes, primarily applied to cases involving adult victims, falls short in fully acknowledging adult victims as victims. [83] Consequently, the lack of complete recognition of adult victims as victims serves as evidence that existing attitudes within courts and investigative authorities have not undergone significant improvement.

Moreover, the Act clarifies that individuals who distribute sexually exploitative photographs or videos obtained without the subjects " consent, even if the subjects themselves took the images, will be subject to punishment. [84] Additionally, those who seek to profit from the illicit filming or dissemination of such photographs will face imprisonment for a specified term, which now surpasses the previous maximum sentence of seven years. [85], [86]. Furthermore, the revised law expands the scope of legal action to include individuals in possession of, purchasing, storing, or viewing illegally obtained sexual photographs or videos, whereas previously only those involved in distribution, sale, leasing, or provision of illicit footage were liable to punishment. [87]

In addition to these modifications, several newly introduced provisions deserve attention. They maintain that a person intimidates another person by using photograph or its duplicates (including a duplicate of the duplicate) which may cause sexual desire or shame shall be punished by imprisonment for at least one year and that any person who interferes with the exercise of a person's right by intimidation or has the person to the work not obligatory for him/her shall be punished by imprisonment with labor for at least three years. [88] Another provision states that individuals who plan or conspire with the intention of committing rape or sexual assault can now be subjected to a maximum of three years of imprisonment, even if they did not directly perpetrate the crime. These newly inserted provisions specifically aim to address the methods employed in the Nth Room case, wherein victims were coerced through the use of their own photos, and to hold lower-level administrators accountable for their role in facilitating the operations of higher-level administrators such as Cho or Moon in establishing the illicit chat rooms. Nonetheless, a critical question remains regarding the prosecution of bystanders whose actions may not amount to the level of planning or preparation for rape or sexual assault against the victims, despite their presence in the chat rooms and their failure to intervene, thereby contributing to the perpetuation of the sex slave network.

The Act on Regulation and Punishment of Criminal Proceeds Concealment underwent significant amendments, introducing several new provisions including Article 10-4, which establishes guidelines for calculating the criminal proceeds associated with cybersex crimes. [89] Article 10-4 stipulates that the criminal proceeds acquired by the offender during the commission of the

68. Kim, *supra* note 62.
69. Seongpongnyeokcheobeolbeop [Act on Special Cases Concerning the Punishment of Sexual Crimes 2020] art. 3, partially amended by Act. No. 17507, Oct. 20, 2020 (S.Kor.). (" A person commits special rape if they commit rape, imitative rape, indecent act by compulsion, quasi-rape, or quasi-indecent act by compulsion in the course of committing intrusion upon habitation, compound larceny, special larceny, or attempt of larceny or robbery. ").
70. *Id.* at art. 3(1), 4(1)-(2), 7(3) & 11.
71. *Id.* at art. 3(1).
72. *Id.* at art. 4(1).
73. Seongpongnyeokcheobeolbeop [Act on Special Cases Concerning the Punishment of Sexual Crimes 2019] art. 3(1), partially amended by Act. No. 16445, Aug. 20, 2019 (S.Kor.).
74. *Id.* at art. 7(3).
75. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 7(3).
76. *Id.* at art. 11.
77. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 11.
78. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 13.
79. *Id.*
80. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 13.
81. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 14.
82. Go-eun Park, *" You Remove It But It Keeps Coming Back " : New Laws Leave Adult Digital Sex Crime Victims Little Recourse*, Hankyoreh (Dec. 12, 2021), https ://english.hani.co.kr/arti/english_edition/e_national/1022931.html.
83. *Id.*
84. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 13.
85. Act on Special Cases Concerning the Punishment of Sexual Crimes 2019, at art. 14(3).
86. Act on Special Cases Concerning the Punishment of Sexual Crimes 2020, at art. 14(3).
87. *Id.* at art. 14(4).
88. *Id.* at art. 14(3).
89. Beomjoesuigeunnikgyujebeop [Act on Regulation and Punishment of Criminal Proceeds Concealment] art. 10-4, partially amended by Act. No. 17263, May 19, 2020 (S.Kor.).

crime shall be presumed as the illicit gains, taking into account factors such as the amount of the proceeds, the timing of property acquisition, and other relevant circumstances ; if there is a reasonable possibility that the criminal proceeds were obtained through the perpetration of the same crime, they shall be presumed as the proceeds related to that particular offense. [90] This amendment carries significant implications as it addresses the historical challenge of establishing a direct correlation between cybersex crimes and the profits generated, thereby facilitating the seizure of criminal proceeds. [91] By easing the burden of proof, these new provisions enable a more effective demonstration of the relationship between these crimes and the associated criminal profits. [92]

The Act on the Protection of Children and Youth Against Sex Offenses have also been revised, marking a crucial milestone in safeguarding minors from cyber violence against women and girls (" VAWG "). Particularly significant is the alteration of the term " child and adolescent pornography " to " child and adolescent exploitation material. " [93] This revision represents an important shift in recognizing the vulnerability and protection needs of minors affected by cyber VAWG. [94]

The Act on the Protection of Children and Youth Against Sex Offenses encompasses notable enhancements in penalties concerning the production and distribution of child and adolescent exploitation material. These amendments are accompanied by provisions for imposing aggravated punishment on repeat offenders, thereby emphasizing the gravity of such offenses. [95] An admirable initiative has been introduced, wherein individuals who report crimes related to this matter are eligible to receive cash prizes. [96] This commendable provision not only serves as an incentive to promote the welfare of minors but also offers investigative authorities an additional avenue for combating the sexual exploitation of children. However, it is important to acknowledge that the effectiveness of this new cash prize provision in detecting and preventing cyber VAWG may be hindered by the low rate of prosecutions for digital sex crimes and the lenient nature of punishments, as highlighted by the CEDAW Committee in 2018. [97] Consequently, careful monitoring of the provision's impact is crucial for evaluating its efficacy in addressing this issue.

Furthermore, a significant addition to the Act is found in Article 7-6, which specifies that individuals involved in the preparation or conspiracy to commit crimes such as rape or indecent act by force against children and adolescents can be subjected to a maximum imprisonment term of three years. [98] This particular provision aims to proactively prevent such offenses by deterring potential perpetrators.

In relation to the Act on Promotion of Information and Communications Network Utilization and Information Protection, a noteworthy legislative measure known as the Deepfake Prevention Law was passed during the National Assembly plenary session, introducing several amendments to the act. [99] Primarily, the amendment mandates the Ministry of Science and ICT to actively promote the development and dissemination of technologies capable of accurately identifying false audio and visual content. [100]

Moreover, an additional provision has been incorporated into the act, requiring information and communication service providers to designate a responsible individual accountable for preventing the distribution of illegal filming material. [101]

Regarding the Telecommunications Business Act, its revision now compels internet service providers to promptly remove sexually exploitative images as defined in Article 14 of the Special Act on Punishment of Sexual Crimes. [102] Nonetheless, despite this amendment, the law still exhibits two significant loopholes : it 1) vaguely defines the " technical and managerial " measures providers are meant to take [103] and 2) is enforceable only for open online forums, allowing offenders to circumvent the law by using private forums instead. [104] These loopholes necessitate urgent attention and rectification to ensure its effectiveness in combating the proliferation of sexually exploitative content.

2° Other Legal Frameworks

13 - The new regulatory developments in the field of AI (such as the Draft EU AI Regulations and the White House's blueprint for an AI Bill of Rights of 2022) show that as digital technology becomes ubiquitous, it will be impossible to regulate it in isolation to other bodies of domestic, regional, and international law. [105] Although not exhaustive, this section maps laws which attempts to address coded gender-based violence in different ways so as to understand how States are attempting to tackle this continually emerging forms of coded gender-based violence. I examine recent reformist agendas in different jurisdictions. In the UK, the Crown Prosecution Service on online violence against women has recommended :

> The landscape in which VAWGCrimes are perpetrated is changing. The use of the Internet, social media platforms, emails, text messages, smartphone apps (for example, WhatsApp and Snapchat), spyware and GPS (Global Positioning System) tracking software to commit VAWG offences is rising. Online activity is used to humiliate, control and threaten victims, as well as to plan and orchestrate acts of violence. [106]

The South African government explicitly acknowledged online gender-based violence in the National Strategic Plan on Gender-Based Violence and Femicide. [107] In the plan, the South African government announced plans to conduct studies on the impact of online violence against women and roll out cyber violence awareness programs and strategies to respond to online gender-based violence.

On December 21, 2020, Lebanon became the first Arab country to pass a law criminalizing online sexual harassment. The law also

90. *Id.*
91. Kim, *supra* note 62.
92. *Id.*
93. Cheongsonyeonseongbohobeop [Act on the Protection of Children and Youth Against Sex Offenses] art. 2(5), 12 & 17, partially amended by Act. No. 17352, June 9, 2020 (S.Kor.).
94. Park, *supra* note 82.
95. Act on the Protection of Children and Youth Against Sex Offenses, at art. 11.
96. Act on the Protection of Children and Youth Against Sex Offenses, at art. 59(1).
97. CEDAW, *Concluding Observations on the Eighth Periodic Report of the Republic of Korea*, [para] 22(c), CEDAW/C/KOR/CO/8 (Mar. 14, 2018).
98. Act on the Protection of Children and Youth Against Sex Offenses, at art. 7-6.
99. Jeongbotongsinmangbeop [Act on Promotion of Information and Communications Network Utilization and Information Protection] art. 4-2, partially amended by Act. No. 17358, June 9, 2020 (S.Kor.).
100. *Id.*
101. Act on Promotion of Information and Communications Network Utilization and Information Protection, at art. 44-9 & 76-2.
102. Jeongitongsinsaeopbeop [Telecommunications Business Act] art. 22-5(1), amended by Act. No. 17460, June 9, 2020 (S.Kor.).
103. *Id.* at art. 22-5(2).
104. Eun-Jee Park, *[MAGNIFYING GLASS] Rushed " Nth Room Law " Unlikely to Actually Stop Criminals*, Korea JoongAng Daily (June 2, 2020), https ://koreajoongangdaily.joins.com/2020/06/02/business/indepth/Nth-room-digital-crime-Naver/20200602195600193.html.
105. In 2013, only three U.S. states had revenge porn laws, and a decade later, 48 states do, plus Washington, D.C., Puerto Rico, and Guam. In 2023, three US states (Virginia, Texas, and California) adopted laws on deepfakes. There are significant examples of successful prosecutions in different jurisdictions of such crimes, which could extend to images that have " been altered to appear to show a person's private parts, or a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, " as legislation in Australia recently established.
106. *Social Media and Other Electronic Communications*, Crown Prosecution Service (Jan. 9, 2023), https ://www.cps.gov.uk/legal-guidance/social-media-and-other-electronic-communications.
107. Republic of S. Afr., National Strategic Plan on Gender-Based Violence & Femicide (Mar. 11, 2020). (" Online violence refers to any act of gender-based violence against a woman 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. ")

encompasses harassment that takes place online through social media and other technological mediums. Perpetrators may spend up to four years in prison and pay fines up to fifty times the minimum wage. Despite the importance of the law, there is ambiguity in the laws as to who is deemed a perpetrator and whether platforms could be held responsible for the offense.

In 2014, the Australian Protection from Harassment Act (" POHA ") 2014 extended the substantive definition of harassing behavior to include electronic means and provided more comprehensive protection orders for victims outside intimate relationships. As such, victims are potentially able to obtain a protection order from the courts, after their images have been shared without consent.

In Singapore, the 2014 Protection from Harassment Act focuses on online harassment and prohibits the intentional or reckless issue of a communication that is threatening, abusive or insulting, which is heard, seen or otherwise perceived and likely to harass or cause alarm or distress or instill in a person fear or provoke violence. A 2019 amendment " prohibits the publication of information identifying the victim or a person related to the victim to harass, threaten or facilitate violence against the victim (also known as " doxing. ") "

The Philippines's 2018 Safe Spaces Act defines gender-based online sexual harassment as :

> Any conduct targeted at a particular person that causes or is likely to cause another mental, emotional or psychological distress ; and fear of personal safety ; sexual harassment acts, including unwanted sexual remarks and comments ; threats ; uploading or sharing of one's photos without consent ; video and audio recordings ; cyberstalking and online identity theft.

However, this definition does not include social media platforms, gaming and similarly to South Africa, does not include new forms of AI and synthetic media.

In 2019, the Philippines amended the Anti-Violence Against Women and Their Children Act of 2004 (" Anti-VAPC Law ") to include ICT-related violence. [108] Under the amendment, ICT violence such as " hacking of personal accounts on social media, the use of location data from electronic devices, fabrication of fake information or news through text messages or other cyber, electronic, or multimedia technology " falls under violence against partners and children. The House of Representatives of the Philippines passed House Bill No. 8009 in May 2023 ; the bill will further expand the Anti-VAPC Law to define ICT-related violence as " any act of omission involving the use or exploitation of data or any form of ICT which causes or is likely to cause mental, emotional, or psychological distress or suffering to the woman and/or her children. " [109] The bill expands protection measures to include " the immediate blocking, blacklisting, removal, or shutdown of any upload, program, or application that causes or tends to cause violence against a woman and/or her children. "

The Cyberspace Administration of China (" CAC "), the national Internet regulator and censor for the PRC, has acknowledged cyberviolence in regulatory actions such as the November 2022 Notice on Effectively Strengthening the Governance of Cyber Violence. [110] In the notice, the CAC describes cyberviolence as " publishing illegal information such as insults, slander, privacy violations, and other unfriendly information against individuals, infringing on the legitimate rights and interests of others, and disrupting the normal order of the Internet. "

In April 2023, the CAC proposed Measures for the Administration of Generative Artificial Intelligence Services to address rising issues in generative AI. [111] The proposal places responsibility on generative AI providers (" organizations and individuals that use generative AI to provide services such as chat and text, image, and sound generation ") as producers of the content generated by their products, heightening the responsibility of providers as they can be held responsible for content created by users of their tools. In addition, generative AI providers assume statutory responsibility of personal information processors when personal information is involved, which confers a duty to protect personal information. Generative AI providers would also be required to take measures to prevent false information and discrimination based on characteristics including gender. However, the proposal does not define ways in which generative AI may discriminate based on gender. The proposal also protects personal information of individuals from being used without consent and requires providers to guide users to not use the generated content to damage the image and reputation of others. Providers found in violation of the proposal are subject to punishment according to relevant law, such as the Personal Information and Protection Law of the People's Republic of China.

In 2020, South Korea introduced the Framework Act on Intelligent Informatization, a social impact assessment on intelligent informatization services, including AI. [112] State and local governments assess the intelligent informatization services on safety and reliability as well as impacts on information culture, society, and the economy. However, this assessment was introduced only in the public sector ; there is no similar regime for the private sector. The assessment is also limited to general impact on society and individuals' personal information and does not assess discrimination or bias against women.

In response to the death of a female actor following online insults, Japan revised its Penal Code in June 2022 to mandate jail time for up to a year or a fine up to 300,000 yen (approximately $2,150) for online insults (when an individual has insulted another in the public sphere to damage their social reputation). [113] The revision also extended the statute of limitations to three years. However, the Penal Code makes no special provisions for online VAWG.

In 2020, the Law on Women's Access to a Violence-Free Life in Mexico City was amended to extend the notion of violence against women to include any acts carried out through information and communication technologies that threatens the integrity, dignity, intimacy, freedom, and private life, of women or causes psychological, physical, economic or sexual harm or suffering, both in the private and public spheres, as well as any act that causes nonmaterial loss to them and/or their families. Following an increase in online attacks on journalists, Spain developed protocols to provide procedures for journalists' complaints, assessment of online harassment complaints by the newspaper's social media team including the withdrawal of comments from social media platforms, and referral to legal counsel and human resources for the purpose of filing legal actions. Despite these good intentions there is little information on what follow up action has been taken in the aftermath of the passage of this protocol.

108. An Act Amending R.A. No. 9262, Rep. Act. No. 4888 (Sept. 30, 2019) (Phil.), https ://hrep-website.s3.ap-southeast-1.amazonaws.com/legisdocs/basic_18/HB04888.pdf.

109. Jean Mangaluz, *House Bill Defining Online Abuse vs Women, Children Hurdles Final Reading*, Inquirer (May 22, 2023, at 11 :43 PM), https ://newsinfo.inquirer.net/1772911/bill-defining-online-abuse-against-women-and-children-hurdles-final-reading-in-house.

110. *Notice on Effectively Strengthening the Governance of Cyber Violence*, Office of the Central Cyberspace Affairs Commission (Nov. 4, 2022, at 19 :10), http://www.cac.gov.cn/2022-11/04/c_1669204414682178.htm.

111. Notice of the Cyberspace Administration of China on Public Comments on the " Administrative Measures for Generative Artificial Intelligence Services (Draft for Comment) ", Office of the Central Cyberspace Affairs Commission (Apr. 11, 2023, at 12 :51), http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm.

112. Jeong Jonggu, *Introduction of the First AI Impact Assessment and Future Tasks : South Korea Discussion*, 11 Laws 73 (2022).

113. *Japan Introduces Jail Time, Tougher Penalties for Online Insults*, Kyodo News (July 7, 2022, at 00 :004), https ://english.kyodonews.net/news/2022/07/1590b983e681-japan-to-introduce-jail-time-tougher-penalties-for-online-insults.html.

The 2022 reauthorization of the United States Violence Against Women Act (" VAWA "), 1994 (As Amended) Subtitle M-Strengthening America's Families by Preventing Violence Against Women and Children included :

> [E]stablishing a federal civil cause of action for individuals whose intimate visual images are disclosed without their consent, allowing a victim to recover damages and legal fees ; creating a new National Resource Center on Cybercrimes Against Individuals ; and supporting State, Tribal, and local government efforts to prevent and prosecute cybercrimes, including cyberstalking and the nonconsensual distribution of intimate images.

This new provision in the reauthorization of the VAWA is welcome and helps build the law as a living document which needs to dynamically address new forms of violence that have been given name to, since its first adoption in 1994.

Apart from national efforts, there are supranational and multinational effort to address online harassment and abuse. The U.S., together with Denmark, Australia, the U.K., and Sweden, launched the Global Partnership for Action on Gender-Based Online Harassment and Abuse during the 2022 meeting of the UN Commission on the Status of Women. [114] This multinational initiative will align countries, international organizations, and civil society to prioritize, understand, and address technology-facilitated gender-based violence.

Although not all forms of isolated acts of technology driven gender-based violence can meet a legal threshold, we need to see them as parts of a continuum of violence against women and underrepresented groups. The 2020 case of Buturuga v. Romania [115] was the first case in which the European Court of Human Rights recognized technology facilitated privacy invasion by an ex-spouse as a form of violence. Violence against women as coercive control needs to be framed through the strengthening of human rights standards and critical information theory. Much like how in the 1970's legal advocates named the field of domestic violence, technology facilitated violence against women must be named so legal remedies can be created for those affected by this offense.

CONCLUSION : NEW DIRECTIONS

14 - Given the rapid growth of technologies, we have entered a new cultural moment, where LLMs and generative AI have the potential to reshape the way we learn, engage, and interact. This moment gives us pause to question whether law has the capacity and agility to keep pace with the ever-changing parade of new technology and their potential to be misused as tools of coded violence against women. I turn in this section to two broad based recommendations.

First, how can Environment, Social and Governance (" ESG ") activities help in addressing digital violence ? The focus on ESG activities has been dubbed the " new paradigm for business. " The corporate social responsibility movement, a forerunner to ESG, spurred the U.S. to enact the Comprehensive Anti-Apartheid Act of 1986, which imposed sanctions and prohibited U.S. nationals from making any new investments in South Africa during the apartheid regime. [116] Similarly, the ESG movement must spark transformative action on ending gender inequality. One way to do this is to mainstream women's human rights norms into ESG. The CEDAW is an inalienable standard of conduct whereby businesses are held accountable to rights violations with corresponding remedies for restitution. However, even when mainstreamed into ESG, these rights must be upheld regardless of their value for business success.

Recent momentum on the " S " in ESG was spurred by the 2018 #MeToo anti-sexual harassment movement and provides a narrative arc for the integration of international women's human rights and intersectional rights into ESG. The 2020 Black Lives Matter movement further shined a spotlight on diversity, equity, and inclusion, as did the Stop Asian Hate movement. The confluence of the global public reckoning on social justice with the COVID-19 pandemic has increased renewed awareness and attention of the role of business in inclusion and human rights.

One way in which investors have tried to address institutional sexism is by putting pressure on corporations to select diverse directors on their Boards. In 2021, the Nasdaq Stock Exchange received approval from the U.S. SEC to adopt a Board Diversity Rule, a disclosure standard designed to encourage a minimum board diversity objective for companies and provide stakeholders with consistent, comparable disclosures concerning a company's current board composition. Having more women on boards in technology companies may drive emerging technologies to address the impact of new technologies on women.

Moreover, recently, the UN OHCHR B-Tech Project released guidance in rights respecting investment in digital technology companies in 2021. [117] This would help incentivize tech innovators to develop codes of ethics for AI and other new technologies that uphold the primacy of women's human rights. The same year saw UNESCO adopting Recommendations on the ethics of AI. The Recommendations call for guardrails and impact assessments and recognize that the rapid rise of AI creates great promise in many areas, including in healthcare, education and climate change, but also raises profound ethical concerns of human rights violations. [118] A human rights-based approach that also includes the Guiding Principles on Business and Human Rights is an important tool to evaluate the effectiveness of these new guidelines.

Although the business case for gender equality is now well recognized, I argue that the CEDAW and women's rights are inalienable and must be guaranteed regardless of their value to the business case. I argue for a more prescriptive and less indeterminate idea of international women's human rights in business. The CEDAW calls upon states to hold business entities accountable to women's human rights. In fact, CEDAW's Article 2(e) calls upon states parties to " take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise[.] " [119]

Second, for a newer understanding of solutions, I turn yet again to the role of Critical Information Theory. Although not mentioned by name, this theory is alluded to in the submission by the " Internet Democracy Project " on online violence against women in India to then-UN Special Rapporteur on Violence against Women, Dubravka Šimonovic. The Project recommended that what was needed was not more laws but more discourse to address online violence :

> What is primarily needed in India, therefore, is more discourse, more awareness and a variety of non-legal measures, so as to challenge and ultimately displace these socio-cultural norms. We believe that measures to tackle online abuse must go

114. Press Release, U.S. Dept. of State, 2023 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse (Mar. 28, 2023), https ://www.state.gov/2023-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/.
115. European Court of Human Rights, Buturuga c. Roumanie, n° 56867/15, 11 February 2020, BUTURUGA c. ROUMANIE (coe.int).
116. Comprehensive Anti-Apartheid Act of 1986, Pub. L. No. 99-440, 100 Stat. 1083 (1986).
117. U.N. Hum. Rts. Off. of the High Comm'r, Rights-Respecting Investment in Technology Companies (Jan. 2021), https ://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B-Tech-Briefing-Investment.pdf.
118. *UNESCO's Recommendation on the Ethics of Artificial Intelligence : key facts* (June 1, 2023), https ://unesdoc.unesco.org/ark :/48223/pf0000385082.
119. G.A. Res. 34/180, Convention on the Elimination of All Forms of Discrimination Against Women, art. 2 (Dec. 18, 1979).

> hand-in-hand with measures to protect women's expression. [120]

This comment raises several important points : first, that discourse on the threats of coded gender-based violence is as important as new laws to address the challenge ; second, that measures to combat online violence must co-exist with the protection of women's freedom of expression rather than with the forced removal of women from the online space.

In balancing this nuanced argument, I would argue that new gender-based violence laws address the orthodoxy of gender-related power relations as a structural or root cause of violence. For example, Nicaragua's Comprehensive Act on Violence against Women and the Reform on Criminal Code (Act No. 641) call for " an education that eliminates the stereotypes of male supremacy and the macho patterns that generated their violence. " [121]

In the final analysis, the idea of digital gender-based violence gives rise to the assumption that algorithms are mathematical models and outside of the control of human behavior. That is far from the truth.

Gender bias in algorithms developed by mostly male technologists drive the programs and platforms that reproduce and reinforce violence against women and recreate a vicious feedback loop. To break this misogynistic cycle of coded violence, we need both law reform and cultural reform. The US Violence against Women Act encodes a humanistic form of male behavior :

> Engaging Men as Leaders and Role Models : To develop, maintain or enhance programs that work with men to prevent domestic violence, dating violence, sexual assault, and stalking by helping men to serve as role models and social influencers of other men and youth at the individual, school, community or state-wide levels. [122]

This provision calls upon male technologists, programmers, developers, and users of technology to rise to the role of leaders, role models, and humanists who can be stakeholders in the prevention on technology driven violence. Toward this end, new and revised gender-based violence laws must adopt a two-pronged approach based in both human rights and Critical Information Theory to address this growing form of violence.■

120. Letter from Anja Kovacs, Dir., Internet Democracy Project, to Dubravka Šimonovic, Special Rapporteur on Violence against Women (Nov. 2, 2017), https ://cdn.internetdemocracy.in/idp/assets/downloads/reports/un-srvaw-report/Internet-Democracy-Project-Submission-Online-VAW-2-November-2017-4.pdf.

121. Comprehensive Act against Violence towards Women (Act No. 779) and the reform of the Criminal Code (Act No. 641), art. 19., A/HRC/WG.6/19/NIC/1, para. 67 (2012).

122. Violence Against Women Reauthorization Act of 2013, §§ 402(a)(b)(3).