

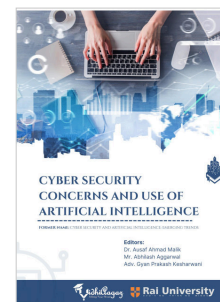
CHAPTER 11

Unvieling the Darknet: Cybercrimes and their Impact on Vulnerable Groups in the Digital Divide

Niyathi S. and Kanigasri Vijayakumar

in *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (VidhiAagaz 2024), pp. 97–101

ISBN 978-81-947620-5-8



CITATIONS

BLUEBOOK (21ST ED.)

Niyathi S. & Kanigasri Vijayakumar, *Unvieling the Darknet: Cybercrimes and their Impact on Vulnerable Groups in the Digital Divide*, in *CYBER SECURITY CONCERNS AND USE OF ARTIFICIAL INTELLIGENCE* 97 (Ausaf Ahmad Malik, Abhilash Aggarwal & Gyan Prakash Kesharwani eds., VidhiAagaz 2024).

OSCOLA (4TH ED.)

Niyathi S. and Kanigasri Vijayakumar, 'Unvieling the Darknet: Cybercrimes and their Impact on Vulnerable Groups in the Digital Divide' in Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani (eds), *Cyber Security Concerns and Use of Artificial Intelligence* (VidhiAagaz 2024) 97.

CHICAGO (17TH ED.)

Niyathi, S., and Kanigasri Vijayakumar. "Unvieling the Darknet: Cybercrimes and their Impact on Vulnerable Groups in the Digital Divide." In *Cyber Security Concerns and Use of Artificial Intelligence*, edited by Ausaf Ahmad Malik, Abhilash Aggarwal and Gyan Prakash Kesharwani, 97–101. Maihar: VidhiAagaz, 2024. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-11/>.

APA (7TH ED.)

Niyathi, S., & Vijayakumar, K. (2024). Unvieling the darknet: Cybercrimes and their impact on vulnerable groups in the digital divide. In A. A. Malik & A. Aggarwal & G. P. Kesharwani (Eds.), *Cyber security concerns and use of artificial intelligence* (pp. 97–101). VidhiAagaz. <https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-11/>

SOURCE

<https://vidhiaagaz.com/books/cyber-security-concerns-and-use-of-artificial-intelligence/chapter-11/>

RIGHTS

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

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

UNVEILING THE DARKNET: CYBERCRIMES AND THEIR IMPACT ON VULNERABLE GROUPS IN THE DIGITAL DIVIDE

Niyathi S.¹³ and Kanigasri Vijayakumar¹⁴

ABSTRACT

In the grooming era of the internet, where access to numerous resources is readily available, the cybersecurity of such accessibility is at risk. The dark web is an anonymous network that connects users by using non-standard and often illicit protocols. It is an end-to-end encrypted network that hides user's identities, giving them a false sense of security. This anonymity is further enhanced by technologies such as Onion routing, the Tor web browser, and Virtual Private Networks (VPNs). The primary reason people use such browsers is that they enable access to the dark web while maintaining user anonymity. The dark web is often exploited for purposes such as identity theft, sextortion, the sale of illicit goods (weapons, narcotics, stolen data, etc.), and as a communication platform for extremist groups to express their oppressive views. It is also a hub for revenge porn, contract killings, and assassinations. The victims of such distressing offenses are often the vulnerable groups such as children, women, elderly population, people residing in rural areas as well as low-income communities. However, they are not only the victims, but also form a significant portion of the perpetrators due to the vicious cycle of poverty, lack of access to education and unemployment. The underlying cause of the issue is the digital divide, which is essentially the proportionate gap between the people who have access to the digital world and those who do not. Digital divide can stem from geographical, socio-economical, global and gender disparities. This paper aims to address such issues that require a multifaceted approach bridging the gap in the digital divide and proposing a solution of having a constructive legal framework and efficient mechanisms to monitor deviations.

Keywords: Dark web, Cybersecurity, Digital divide, Sextortion, Vulnerable groups

INTRODUCTION

Amidst the rapid evolution of digital technologies, cybercrime has emerged as one of the most pervasive and insidious threats to global security, challenging the very foundations of privacy, trust, and governance in the modern world. Dark web traces back to the 2000s, when it was only there for ethical purposes and legal usage. However, as awareness of the power of cyberspace grows, many individuals choose to misuse it for personal gain rather than considering its broader societal implications. With the advent of emerging technologies like Artificial Intelligence and Extended Reality (XR), users are increasingly exploiting the opportunities within the once-sacred digital realm, drawing themselves into unethical practices with the internet as their primary tool. The research aims to address the malefactions such as sextortion, revenge porn, illegal trafficking and sale of illicit goods online and various other crimes arising in the digital world. The main objective is to educate the vulnerable groups in order to bridge the gap of digital divide that persist amongst them. The same technology that has been the root cause of these problems can also be harnessed to prevent such crimes and create a safer cyberspace, where individuals can freely express their views and opinions, legitimizing the responsible use of the internet. Furthermore, the evolving potential of technology offers innovative solutions to combat these illicit activities and address their perpetrators effectively. The paper argues the fact that the vulnerable

¹³ Student at Vellore Institute of Technology, Chennai, India.

¹⁴ Student at Vellore Institute of Technology, Chennai, India.

groups are the major victims and are not protected due to lack of knowledge, awareness and absence of effective legislative framework exploiting their social and economic stance in the society.

LITERATURE REVIEW

The United Nations Development Programme (UNDP) report on ‘Cyber Violence Against Women and Girls’ aims to highlight the various forms of cyber violence against women and girls (VAWG), especially those linked to intimate partner violence (IPV), while emphasizing the disproportionate impact on women. It advocates for a comprehensive understanding of cyber VAWG as part of a continuum of violence that includes offline experiences, calling for more research into the effects on victims. However, the report overlooks significant legal ambiguities. Defining cyber VAWG as a form of VAW may encounter legal challenges, as existing laws often fail to address online behaviours, leading to confusion in enforcement and accountability. Additionally, both policymakers and the general public may lack a full understanding of the complexities of cyber VAWG, resulting in underreporting and inadequate responses. Furthermore, women from diverse backgrounds may experience cyber VAWG in varying ways, hence the one-size-fits-all approach neglects the specific needs of marginalized groups.

1. Online Gender-Based Violence against Women and Children:

According to the 2022 report of National Crimes Record Bureau (NCRB), instances of cybercrimes against women and minors have escalated by 32 percent compared to the previous year. Cyberviolence seems to have bias towards women and girls, who constitute a major section of the vulnerable group and tend to get exposed online. Recent data from the NCRB, unveiled a concerning picture regarding cybercrimes against children. This issue particularly affects those who face multiple social disadvantages, including race, class, caste, religion, and disability. Women of colour are especially vulnerable to online violence, as are those from ethnic or religious minorities, as well as lesbian, bisexual, transgender, or intersex (LBTI) women, who often face harsh criticism on social media. Peer-inflicted online abuse is not limited to young people; it also targets women in positions of power. This abuse often acts as a mechanism of control, aimed at those who challenge patriarchal norms and advocate for gender empowerment. Although the Information Technology Act of 2000 was the first legislation to address IT crimes, it had shortcomings, leaving the country without a robust legal framework to combat cybercrime against women. During the pandemic, online gender-based violence surged globally, and many countries struggled to address violations against women's online safety due to inadequate legislative measures.

In the case of *Shreya Singhal v. Union of India*, two women faced charges under Section 66A of the Information Technology Act of 2000 for allegedly posting offensive comments on Facebook regarding the city of Mumbai's response to a politician's death. This section aimed to penalize individuals for sending grossly offensive or false information via digital platforms, which could cause annoyance or harm. The case attracted significant media attention, prompting the Supreme Court to declare Section 66A unconstitutional, ruling that it violated the right to freedom of speech and expression under Article 19(1)(a) of the Constitution. The court criticized the section's vague language and potential for arbitrary

arrests, emphasizing its "chilling effect" on free expression. While this judgment marked a victory for digital freedom, it highlighted a gap in the legal framework for addressing cyber harassment and online abuse.

The research proposes strategies to close the gender gap in technology access by fostering equal employment opportunities for economic empowerment, social integration, and sustainable development, thereby ensuring women's full engagement in the digital economy. By prioritizing an inclusive tech ecosystem, we can enable marginalized groups—especially women and other underrepresented communities—to contribute to innovative solutions that meet the rising demands of the digital economy. There is need for a robust legal framework that deals with cyberviolence with special emphasis towards women and children.

2. Deepfake technology and its Ethical impacts:

Deepfakes are videos created using deep learning, AI, and image manipulation techniques to fabricate events, often with the intent to spread misinformation. Technologies like Generative Adversarial Networks (GANs) and Machine Learning (ML) work in tandem to generate such videos. The first major incident which involved deep fakes occurred in 2017, when a Reddit user named "DeepFakes" posted adult videos that exposed the faces of celebrities onto the bodies of porn stars. While this wasn't initially classified as an attack, it caused widespread outrage and raised serious concerns about privacy violations and the need for effective deepfake detection. In response to this, Reddit and other social media platforms banned the content and the user, leading some legislative bodies to propose laws targeting deepfake pornography and the unauthorized use of individuals' likenesses. According to a report by global security software company McAfee, approximately 22% of Indians had encountered political deep fakes, which they later realized was false. 55% of the respondents expressed concern about the potential for cyberbullying through deepfakes, and 52% were worried about the creation of fake pornographic content. High-profile individuals are often the targets of deepfake manipulation. For instance, actor Ranveer Singh filed a police report after a deepfake video falsely showed him endorsing a political party and criticizing Prime Minister Narendra Modi during a news interview. Similarly, actress Rashmika Mandanna was also victimized, as her face was misused in inappropriate videos that damaged her image and reputation. These incidents are becoming increasingly frequent and warrant immediate attention.

Through this research we propose stringent regulatory measures to ensure that the inbuilt algorithms in deepfake or AI aided software are not biased and ensure that the data is end-to-end encrypted to maintain privacy. There is further a need for enhanced deepfake deduction technologies which will help track corrupt users to avoid any mishap. The rising concerns in the area of deep fake calls for an effective legislation in order to deal with such issues and come up with quick measures.

3. The Role of Social Media in the Proliferation and Prevention of Revenge Porn:

According to a survey conducted by the Cyber and Law Foundation and an NGO, about 27% of internet users in India aged 13 to 45 have been victims of revenge porn and sextortion. In a conservative country like India, the victim's first thought is often to avoid filing a complaint or, tragically, to consider

suicide due to societal judgment. The legal process has primarily concentrated on the technicalities of content removal, neglecting the emotional and psychological trauma experienced by the victim. This highlights a systemic flaw in how online harassment cases are handled, which often overlooks victim support and their counselling. This can be further understood through the case of *Mr. X and Ors. Vs Union of India*, where the petitioner sought the removal of her non-consensually shared explicit images from online platforms like Google. The perpetrator, posing as a British chartered accountant, manipulated her and her son to extort money through threats. While this case prompted stricter enforcement for removing non-consensual content, it revealed India's lack of cohesive legislation against revenge porn, sextortion and image-based abuse. Despite reporting the issue to authorities and platforms, timely action was not taken to remove the images, underscoring the slow response of intermediaries and the absence of preventive measures to stop content from reappearing online. The non-consensual distribution of intimate images and videos is a troubling issue that has been intensified by the rise of unmoderated instant messaging platforms like Facebook, Telegram, Instagram, YouTube etc. The combination of anonymity and a relaxed regulatory environment has enabled the growth of social media, its channels, and bots that share such content. This trend poses significant ethical and mental health risks and demands urgent intervention.

Through this paper we would like to propose a mechanism designed to map the complex network of social media spaces involved in non-consensual pornography and to identify even slightly modified copies of images circulating in various channels and groups. While these platforms do have community guidelines that prohibit sharing explicit content, enforcement is often inconsistent, and the process for removing such content can be slow. Hence a proper efficient framework coupled with effective redressal in the review process of concerned social media should be implemented.

4. Protection of Youth from XR (Extended Reality) Online Gaming Platforms:

The future of Extended Reality (XR) and gaming is a topic of significant interest, with experts predicting far-reaching impacts on society, entertainment, education, and various industries. By 2040, the metaverse—a shared digital environment—is expected to transform human interaction through immersive experiences that blend physical and digital realities. XR technologies, including virtual reality (VR) and augmented reality (AR), will play a key role, offering spaces for socializing, education, and more. The advent of online gaming has been impacting youth since 2017, when the "Blue Whale Challenge" emerged. A 14-year-old student from Andheri in Mumbai was the first victim of the game to be reported in India. The Blue Whale Challenge is an online game that originated in Russia, notorious for its dark and dangerous nature. It involves players being assigned a series of tasks or dares by a "curator" over 50 days. The initial tasks are relatively simple, such as "wake up in the middle of the night" or "watch a scary movie." However, the challenges progressively become more dangerous, with instructions like "stand on the edge of a tall building" or "carve a whale into your arm." The final challenge tragically compels the player to take their own life. Cybercriminals can use VR environments to identity theft, phishing, or fraud by creating deceptive virtual spaces. XR can also be misused for virtual harassment, bullying, or stalking within immersive platforms. As XR evolves, so do its protection and security vulnerabilities, making it a potential target for hackers and other malicious

actors. The Ministry of Home Affairs (MHA) has issued a warning about frauds related to gaming apps, urging users to exercise caution while engaging in online gaming. The Indian Cyber-Crime Coordination Centre (I4C), part of the MHA's Cyber Wing, has advised users to download apps only from trusted sources, verify the legitimacy of game app publishers, and avoid falling for in-app purchases and subscription scams. As of the year of 2022, the Centre had blocked 581 apps, including 174 betting and gambling platforms and 87 loan lending apps, based on recommendations from the MHA. These apps, blocked under Section 69A of the IT Act, 2000, included popular gaming platforms like PUBG and Garena Free Fire. Many of the betting apps collected UPI payments through proxy bank accounts, with the funds being routed through hawala, cryptocurrency, and other illegal means. Recently, Union Home Minister Amit Shah confirmed that over 500 internet-based applications have been blocked on I4C's recommendation.

Through this research we would like to point out that the National Gaming Commission which overlooks into matters of e-gambling should also emphasise on those applications involving XR, VR and AR, and shall prescribe boundaries within which the algorithms can be used to develop such games. This will ensure that the apps are not violent in nature thereby protecting mental and psychological health of users. The developers must focus on utilising these notable technologies in the field of criminological research, medical training for medical practitioners, surgical simulations and to foster mental health treatment in order to reduce their dependence on unethical human experimentation.

CONCLUSION

Cyberspace has been developing at a rapid pace in the digital era however it falls short on certain aspects such as cyber bullying, online gender-based harassment, sextortion, revenge porn, misuse of deepfake and XR (Extended Reality) which tends to pose a serious problem in the society. This research emphasizes the urgent need to close the gender gap in technology access, advocating for an inclusive digital economy that empowers marginalized groups, especially women. We propose a framework to track social media networks related to non-consensual pornography, improve enforcement of content guidelines, and expedite harmful content removal. Additionally, we call for stringent regulations to ensure unbiased algorithms and secure data encryption in deepfake technology, alongside enhanced detection tools to identify malicious users. We also urge the National Gaming Commission to oversee XR, VR, and AR applications to prevent violent content and protect mental health. These recommendations aim to foster a safer and more equitable digital landscape.
