

Understanding Gender-Based Cybercrime from a Sociological Perspective

K.A.D.S Herath

University of Ruhuna, Sri Lanka,

A. D. Nirosha Ruwanpathirana

University of Jayewardenepura, Sri Lanka,

and

E.A.D. Anusha Edirisinghe

University of Kelaniya, Sri Lanka.

Abstract

Cybercrimes can be identified as the dark shadows cast by the brilliance of technological advancement. Invisible digital technology is connecting with humans in an unprecedented way and has become a global social problem that transcends borders and challenges traditional concepts. The objectives of this research are to understand the social factors that affect gender specific cybercrimes, analyse the disparities in them and the way they affect individual victimisation in the legal aspect. Using a purposeful sampling method in a qualitative research methodology, the primary and secondary data obtained have been analyzed thematically according to a sociological perspective using feminist theory, reaction theory, social control theory and labelling theory. This analysis confirms that sociocultural norms play a crucial role in shaping the power dynamics of cyberspace, that patriarchal structures that extend to the digital space make women vulnerable, and that technologically human relationships are no longer valued as interpersonal relationships built due to the anonymity of technology that develop into cyberspace crimes. The findings suggest that gaps in legal frameworks and the lack of institutional knowledge to implement them further complicate cybercrime and increase cybercrime. This research suggests that developing legal reforms to effectively address cybercrime, developing an attitude that respects the dignity of others in human relationships, and educating women about the ethical principles of online relationships can prevent cybercrime as a social phenomenon and ensure reliable digital security.

Key words: - Cybercrime, Gender, Legal loops, Social inequality, Victimization

Introduction

The increasing prevalence of technology has significantly changed the way people live socially, as it now transforms what was originally conceived as human-to-human interaction into a form of interaction that occurs remotely over the internet. These changes have made communication faster and more efficient. However, at the same time, social dysfunction and harmful behavior have increased. One of the most troubling is the rise of gender-biased cybercrimes – crimes committed through technological means with a clear female focus on women and gender

minorities because of their identity and gender roles. These crimes, which are a product of online spatial interactions and hierarchies, include cyberstalking, online harassment, defamation, impersonation, and the sharing of intimate images without consent. All of these crimes are perpetuated and exacerbated by the inherent social constructs of gender violence (Gurumurthy et al., 2019).

Examining crime from a sociological perspective reveals not only a violation of the law but also an act of social inequality, the division of power, and the failure of social norms to cohere (Carabein et al., 2020; Durkheim, 1893). Cyberspace, while not technologically embedded, is socially constructed, meaning that it is open to gendered power relations. Gendered violence is facilitated and exacerbated in enduring digital forms of interaction due to anonymity, lack of boundaries, and the inability to erase digital traces (Terkel, 2011; Lyon, 2003). There is a growing body of literature discussing cybercrime from a legal, technological or psychological perspective; however, there has been little attention paid to the sociological frameworks that place certain groups, women specifically, at greater and disproportionate risk. Gender as a social construct influences how social agents are viewed, targeted and treated in the realm of digital space (West and Zimmerman, 1987; Butler, 1990). In Sri Lanka and other South Asian contexts, these digitally enabled gender-based harms are compounded by lax legal frameworks and cultural norms, which provide systemic impunity with enhanced victimization.

This research contributes to the knowledge gap by providing a sociological exploration of gender-based cybercrime in Sri Lanka. This research emphasizes the role of sociocultural norms, laws, and power relations that exist in cyberspace and their configuration of patterns of victimization. The research used feminist theory, labeling theory, social learning theory, and social control theory as lenses to interpret gender-based digital violence as a dynamic of social power relations. The study design used a qualitative methodology that included qualitative case study analysis and expert interviews to thematically analyze cybercrime cases involving female victims, contextualized in real life. The study does so by identifying the structural causes of acts of victimization related to gender-based violence online and attempting to critically assess the practical limitations and inadequacies of legal frameworks in addressing gender-based cyberviolence in Sri Lanka, while illustrating the extent to which reforms are needed from a socially conscious perspective. Finally, this paper contributes to a more complex interpretation of cybercrime as a gendered phenomenon and the need to further incorporate sociological interpretations of digital governance, education, and policy-making processes.

Literature Review

The literature review conducted for this study provides a comprehensive understanding of the phenomenon of gender-based cybercrime by examining existing studies in both international and Sri Lankan contexts. The review identifies key themes, findings, and significant gaps that justify the need for further research from a sociological perspective. Cybercrime is a growing social problem in the digital age that has significant implications for individuals, communities, and nations. Existing studies consistently highlight that women, in particular, are disproportionately affected by cybercrime, including cyberbullying, cyberstalking, doxing, and revenge porn. However, much of the existing literature views these incidents primarily as legal

or psychological issues, with limited exploration of the underlying social structures that contribute to gender-based violence.

Key findings from International Studies and Sri Lankan Studies

Lazarus, Button, and Kapend (2022) examined how socialisation processes shape gendered experiences of cybercrime. Their findings suggest that women may be more vulnerable to digital violence due to internalised fear and subordination embedded in traditional gender roles. Men's socialisation patterns encourage them to resist fear and assert dominance, while women are taught to conform and avoid conflict, making them easier targets for digital abuse. The United Nations Broadband Commission (2015) addresses cyber-violence against women and girls (cyber-VAWG), which it identifies as a global problem that reinforces offline gender-based violence. While emphasising the need for legal, educational, and technological cooperation to create safe online environments, the report does not thoroughly examine the root causes of these crimes. This gap supports the sociological focus of the current study, which seeks to identify the social structures and inequalities that perpetuate gender-based cyber-violence. Chudasama, R., & Gajjar, S. (2023). provide insights into how technological dependency during the COVID-19 lockdown has led to an increase in women becoming cyber-victims. The lack of a strong legal framework further exacerbates the situation, with psychological consequences such as social exclusion and emotional trauma reported. The author calls for social change and legal reform but does not explore the sociocultural drivers of this violence. Dhupdale (2020) presents cybercrime as an evolving war phenomenon, noting that technological advances have outpaced legal developments. He emphasises the need for global cooperation and policy reform but lacks a gender-based analysis. In the Sri Lankan context, researchers such as Jayasekara and Rupasinghe (2015) have explored cybercrimes extensively, focusing on technical and legal challenges. While recognising that both men and women are affected, the study offers limited discussion of why women are disproportionately targeted.

Methodology

In order to understand the persistence of gender-based cybercrime in the absence of legal mechanisms to address it, we'll need to look at sociocultural, legal, and institutional dimensions together. Our study takes a qualitative methodological approach, informed by feminist theory, social learning theory, labelling theory, and social control theory. Together, these provide a multidimensional way of thinking through how gender norms, power relations, and structural inequality relate both to the perpetration of and the response to cybercrime. Qualitative methods are particularly appropriate for studying socially embedded phenomena and enabling the voices of individuals whose experiences have been marginalised to be heard in public discourses.

Sample Selection

Using a purposive sampling technique allowed the researcher to identify individuals with direct and professional experience associated with gender-based cybercrime for the sample. A total of 15 individuals who were either victims, legal professionals, cybercrime investigators, or activists within the community and child protection fields formed the sample. Selection was

based on the following three main criteria: the participants' personal and professional exposure to gender-based cybercrime, knowledge of the Sri Lankan Computer Crimes Act No. 24 of 2007, and willingness to discuss relevant detail in relation to the objectives of the research. The participants were mainly women, aged between 21 and 45, and from an urban or semi-urban context across Sri Lanka. All participants were fully informed about the nature of the research and verbally consented to their participation in the study. Anonymity and confidentiality were maintained following ethical research practices.

Data Collection Approach

Data collection was conducted through semi-structured, in-depth interviews. This approach afforded the researcher some level of control over the conversation while allowing for the participant's experiences and perspectives to be conveyed in detail. Each of the interviews lasted approximately 15-25 minutes. These interviews were conducted face-to-face, by telephone, or via secure online platforms, depending on the participant's preference and safety concerns. Questions focused on personal experiences of cyber victimisation, the efficacy of current legal frameworks, institutional responses to complaints, social stigma, and cultural attitudes and perspectives relating to gender and online conduct.

Data Analysis Techniques

Thematic analysis, as described by Brown and Clark (2006), was used to analyse the interview transcripts for this research. Thematic analysis as an approach assists researchers with identifying and interpreting meaningful patterns across a data set. Thematic analysis consists of a number of steps or phases. The first phase involves familiarising oneself with the transcripts through multiple readings and then creating the initial codes. The initial codes were then grouped into more general areas of themes, were consolidated, randomly reviewed to assess consistency, and regrouped, consolidated, and adapted to maintain commonality throughout the transcripts. Through the process, five key themes emerged from the data: i) targeting of young women through cyberbullying; ii) issues around social status and the digital landscape; iii) traditional gender roles reinforced through cyberspace; iv) an increase in antisocial behaviour owing to the digital environment and the lack of regulatory measures; and v) legal crises for victims, rooted in institutional and legislative gaps. These themes will be detailed in the next analysis section, with the theoretical and contextual framework appropriately put into place.

FINDINGS & DISCUSSION

This section presents the principal findings of the study, organized thematically and interpreted through sociological theories and concepts. The findings are derived from a thematic analysis of 15 case studies of cybercrimes with a gendered nature. These findings are organized into three main areas: cyber harassment against young women, cybercrimes' impact on social status and structure, and the relationship between social power dynamics and the cyberspace. Each theme is discussed with reference to key sociological theories such as Feminist Theory, Labeling Theory, Social Learning Theory, and Social Control Theory, supported by evidence from field data.

Cyber Harassment and the Victimization of Young Women

One of the major findings of this study is the increasing prevalence of cyber harassment targeted at young women, particularly in forms such as cyberbullying, character defamation, online stalking, and sexualized threats. These actions are often facilitated by the anonymous nature of digital platforms and reflect underlying gender power imbalances in society. Field data illustrate instances where women are labeled with derogatory terms such as "prostitute" and publicly shamed on social media. These actions, when analyzed through Labeling Theory (Becker, 1963), demonstrate how victims are socially stigmatized, causing them psychological harm and social alienation. The Feminist Perspective further highlights how women are commodified and subjected to control in patriarchal systems that extend into digital spaces (Schwartz, 1989; Van Velsor & Hughes, 1990).

Additionally, cases reveal how victim-blaming attitudes are reinforced, especially when past relationships are weaponized to justify harassment, as seen in dating-related incidents. This aligns with victimization theory and indicates a structural tolerance for misogyny in cyberspace. For example, anonymous phone threats with sexual content have been used to control and intimidate women, showcasing the digital extension of intimate partner violence. The Social Learning Theory (Bandura, 1977) explains the repeated nature of such crimes, where offenders learn and replicate aggressive behavior via observation and interaction in digital environments. Further, the Social Control Theory supports the notion that the lack of legal enforcement and anonymity weakens social norms, allowing deviant behavior to flourish online.

Social Status and the Impact of Cybercrime

Another prominent theme concerns the differential impact of cybercrime based on individuals' social status. The study finds that individuals with limited economic resources, lower professional power, or marginalized social identities are disproportionately victimized. For instance, women in low-income groups and young schoolgirls were among the most vulnerable to financial fraud, hacking, and revenge pornography. Cybercriminals often exploit victims' social capital (Bourdieu, 1986) by manipulating trust built in digital relationships. In one case, a woman engaged in an online romantic relationship was deceived into financial loss under the guise of receiving a gift. The perpetrator exploited emotional vulnerabilities and economic limitations. Similarly, the study reports a significant number of unauthorized intimate photo sharing incidents, where male partners used shared images for extortion or public shaming after a breakup. Such cases reflect a growing form of digital intimate partner violence (Woodlock, 2017), reinforcing patriarchal control even after the relationship ends. Digital inequality and lack of awareness exacerbate the issue. Victims often do not report due to fear of stigma, loss of reputation, or further victimization, reflecting a deeply rooted cultural silence on digital abuse. This phenomenon supports findings from other sociological research that link gender, class, and technological access to increased digital vulnerability.

Gender Roles in Cyberspace and Social Power Dynamics

A third key finding emphasizes that cyberspace is not a neutral domain but rather a reflection of patriarchal power structures seen in physical society. Gendered power imbalances and patriarchal norms shape how men and women interact in digital environments. Young women, especially in romantic relationships, face heightened risks of coercion and surveillance. Technology such as GPS tracking, password sharing, and social media monitoring is used to control women's behavior, echoing traditional gender expectations in modern digital formats. This trend aligns with the concept of digital patriarchy (Dragiewicz et al., 2018), where technology becomes a tool for enforcing control over female autonomy. The Feminist Theory provides critical insights into these dynamics, arguing that women's online experiences mirror their systemic disempowerment in society. Moreover, intersectional feminism (Crenshaw, 1991) explains that women's digital victimization is compounded by other social markers such as age, race, or class. Digital spaces, though perceived as anonymous and equalizing, are often weaponized to perpetuate patriarchal dominance, with cultural attitudes often normalizing online harassment. Women's bodies and reputations are particularly targeted, creating a hostile environment that severely restricts their participation in online life.

The study confirms that gender-based cybercrimes are a sociological issue rooted in power asymmetries, cultural norms, and structural inequalities. The findings emphasize that: Cyber harassment primarily targets women, especially young women, reflecting gendered violence patterns. Social status influences vulnerability to cybercrime, with those from marginalized backgrounds facing greater risk. Patriarchal power dynamics persist in digital spaces, reinforcing offline inequalities through online behaviors. Sociological theories such as Feminist Theory, Labeling Theory, Social Learning Theory, and Social Control Theory illuminate the underlying mechanisms through which these crimes occur and persist. These findings underscore the urgent need for legal reform, gender-sensitive digital policies, and educational campaigns to foster safer, more equitable digital environments.

Conclusion

This paper offers a thorough sociological analysis of gender-based cybercrime in Sri Lanka, demonstrating how social, cultural, and technological factors influence digital victimisation. The study reveals the lived reality of victims, particularly women, and draws attention to the power dynamics present in cyberspace through a qualitative methodology based on constructivist ontology and interpretivist epistemology. The study identified key themes through the analysis of 15 case studies and interviews with social service and law enforcement professionals. These themes included the normalisation of antisocial behaviour, the impact of social status in cyberspace, and the victimisation enforcement of young women, the role of digital gendered power, the existence of legal loopholes, and online anonymity.

Applying feminist theory, social learning theory, and labelling theory allowed for a more thorough comprehension of the ways in which social norms and structural injustices fuel online harm and women's marginalisation. Stronger legal frameworks, culturally aware law enforcement, and public awareness campaigns that tackle the sociological as well as technological aspects of cybercrime are all urgently needed, according to the research. Finally,

in order to guarantee a more fair and secure online environment for everybody, this study emphasises how critical it is to close the gap between digital policy and social reality.

References

1. Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, NJ: Prentice Hall.
2. Becker, H. S. (1963). *Outsiders: Studies in the sociology of deviance*. Free Press.
3. Bourdieu, P. (1986). "The forms of capital" In J. G. Richardson (Ed.), *Handbook of theory and research for the sociology of education* (pp. 241-258). Greenwood Press.
4. Butler, J. (1990). *Gender trouble: Feminism and the subversion of identity*. Routledge.
5. Broadband Commission for Digital Development Working Group on Broadband and Gender. (2015). *Cyber violence against women and girls: A worldwide wake-up call*. United Nations Broadband Commission.
6. Carabein, J., et al. (2020). *Cybercrime and society*. Sage Publications.
7. Chudasama, R., & Gajjar, S. (2023). "Cyber crime against women", *National Journal of Cyber Security Law (NJCSL)*, 5(2), 45–56. CELNET Publications. (lawjournals.celnet.in in Bing)
8. Crenshaw, K. (1991). "Mapping the margins: Intersectionality, identity politics, and violence against women of color". *Stanford Law Review*, 43(6), 1241–1299
9. Dhupdale, S. S. (2020). "Cybercrime: An evolving war phenomenon", *International Journal of Advanced Research in Computer Science*, 11(5), 45–50.
10. Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2018). "Technology-facilitated coercive control: Domestic violence and the digital patriarchy", *Feminist Media Studies*, 18(4), 609–625.
11. Durkheim, E. (1893). *The division of labor in society*. Free Press.
12. Gurumurthy, A., et al. (2019). "Gender and cybercrime: A study of women's experiences in India", *Journal of Cybercrime & Cybersecurity*, 3(1), 1-15.
13. Jayasekara, A. H. D., & Rupasinghe, W. (2015). "Cyber-crime in Sri Lanka", *Journal of Communication and Computer*, 12(10), 300–307. (doi.org in Bing)
14. Lazarus, S., Button, M., & Kapend, R. (2022). "Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types", *The Howard Journal of Crime and Justice*, 61(3), 381–398.

15. Lyon, D. (2003). *Surveillance as social sorting: Privacy, risk, and digital discrimination*. Routledge.
16. Schwartz, M. D. (1989). "The undercutting edge: A look at the connection between rape and everyday violence" In M. D. Schwartz (Ed.), *Rape and the criminal justice system* (pp. 1-14). Sage Publications.
17. Terkel, S. (2011). *Race: How blacks and whites think and feel about the American obsession*. Anchor Books.
18. Van Velsor, E., & Hughes, M. W. (1990). "Gender differences in the development of managers: Why women managers stay in middle management", *Journal of Vocational Behavior*, 36(3), 262-276.
19. West, C., & Zimmerman, D. H. (1987). *Doing gender*. *Gender & Society*, 1(2), 125-151.
20. Woodlock, D. (2017). "The abuse of technology in domestic violence and stalking", *Violence Against Women*, 23(5), 584-602.

