Understanding Non-Reporting Behaviour in Cybercrime Victimization: An Opinion Study

Jemi Suganthi. A[1], Nagaraj.P. A[2], Barathnathan S[3], Dexin Joyan[4]
[1,2,3]*III B.A Criminology, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India*
[4]*Assistant Professor, Department of Criminology, Nehru Arts and Science College, Coimbatore, Tamil Nadu, India*

***Abstract*—The rapid expansion of digital technology has significantly transformed modern society, enhancing communication, economic activities, and access to information. However, this digital transformation has also led to a substantial rise in cybercrime, affecting individuals across different socio-economic backgrounds. Despite the increasing prevalence of cyber offences such as online fraud, identity theft, cyberstalking, and data breaches, a large number of incidents remain unreported. This phenomenon, often referred to as the "dark figure of crime," presents serious challenges to law enforcement agencies and policymakers.**

This study aims to explore the reasons behind non-reporting behaviour among cybercrime victims through an opinion-based analytical approach. It examines psychological, social, cultural, and institutional factors influencing victims' reluctance to report incidents. Key barriers identified include fear of social stigma, lack of awareness, distrust in authorities, privacy concerns, and the complexity of reporting procedures.

The findings highlight that non-reporting not only distorts crime statistics but also weakens policy formulation and allows offenders to operate without accountability. The study emphasizes the need for improved digital literacy, simplified reporting mechanisms, and stronger institutional support to encourage reporting and enhance cybercrime prevention strategies.

***Index Terms*—Cybercrime, Non-reporting Behaviour, Victimization, Digital Security.**

I. INTRODUCTION

The twenty-first century has witnessed a profound transformation in the way individuals interact, communicate, and conduct everyday activities. With the rapid advancement of digital technology, the internet has evolved from a simple communication tool into a fundamental infrastructure that supports modern society. Activities such as online banking, e-commerce, education, entertainment, and social networking are now deeply integrated into daily life. In countries like India, initiatives aimed at digital empowerment have accelerated internet penetration and increased reliance on digital platforms across urban and rural populations.

However, this digital expansion has also introduced new vulnerabilities. As technology evolves, so too does criminal behaviour. Traditional crimes have extended into virtual spaces, giving rise to cybercrime—a form of criminal activity that uses computers, networks, and the internet as tools, targets, or environments for illegal actions. Cybercrime includes offences such as hacking, identity theft, online fraud, cyberstalking, phishing, and data breaches. These crimes are often characterized by anonymity, speed, and cross-border execution, making them difficult to detect and control.

Despite the growing prevalence of cybercrime, a significant number of incidents remain unreported. This phenomenon, known as non-reporting behaviour, represents a major challenge in the field of criminology. Non-reporting creates a gap between actual victimization and officially recorded data, resulting in what is referred to as the "dark figure of crime." This hidden dimension undermines the effectiveness of the criminal justice system by limiting its ability to respond appropriately.

Understanding non-reporting behaviour is essential for several reasons. Firstly, it affects the accuracy of crime statistics, which are crucial for policy formulation and

resource allocation. Secondly, it allows offenders to operate without accountability, thereby increasing the likelihood of repeated offences. Thirdly, it reflects underlying issues such as lack of trust in law enforcement, social stigma, and insufficient awareness of reporting mechanisms.

This study aims to explore the reasons behind non-reporting behaviour in cybercrime victimization. By examining psychological, social, cultural, and institutional factors, the research seeks to provide insights into why victims choose silence over reporting. Ultimately, addressing this issue is vital for creating a safer digital environment and strengthening the effectiveness of cybercrime prevention strategies.

II. DIGITAL REVOLUTION AND EMERGING CYBERCRIME

The digital revolution has fundamentally altered the structure of modern society. Technological advancements such as smartphones, high-speed internet, artificial intelligence, and cloud computing have created a highly interconnected world. These innovations have enhanced efficiency, accessibility, and communication, allowing individuals and organizations to perform tasks more quickly and conveniently.

However, the same technologies that offer benefits also create opportunities for criminal exploitation. Cybercriminals leverage technological vulnerabilities, human error, and lack of digital awareness to carry out illegal activities. Unlike traditional crimes, cybercrime does not require physical presence. Offenders can operate remotely, often using sophisticated tools such as encryption, malware, and anonymous networks to conceal their identity.

One of the defining characteristics of cybercrime is its borderless nature. Criminals can target victims across different countries, making jurisdiction and enforcement complex. Additionally, the rapid pace of technological change often outstrips the ability of legal systems to adapt, resulting in gaps in regulation and enforcement.

In India, the introduction of the Information Technology Act, 2000 marked a significant step in addressing cybercrime. The Act provides legal recognition to electronic transactions and outlines penalties for offences such as hacking, identity theft, and data misuse. Despite this framework, challenges remain in terms of implementation, awareness, and accessibility.

Another important aspect of cybercrime is its scalability. A single cybercriminal can target thousands of victims simultaneously through phishing emails or malware attacks. This increases the potential impact of cybercrime and makes prevention more difficult.

The digital revolution has also changed the nature of victimization. Individuals are now exposed to risks not only in physical spaces but also in virtual environments. As reliance on digital platforms continues to grow, the likelihood of cybercrime victimization increases.

Therefore, while the digital revolution has brought numerous advantages, it has also created a complex landscape of risks. Addressing these challenges requires a combination of technological solutions, legal frameworks, and public awareness.

III. CYBERCRIME VICTIMIZATION

Cybercrime victimization refers to the experience of being harmed through digital means. Unlike traditional crimes, cybercrime does not always involve physical contact, yet its impact can be equally severe or even more damaging. Victims of cybercrime may suffer financial, psychological, social, and reputational harm.

Financial loss is one of the most immediate consequences of cybercrime. Victims may lose money through online fraud, phishing scams, or unauthorized transactions. In many cases, recovering lost funds can be difficult, especially when the offender operates from another jurisdiction.

Psychological harm is another significant impact. Victims often experience stress, anxiety, fear, embarrassment, and depression. The emotional toll of cybercrime can be long-lasting, particularly in cases involving harassment, stalking, or exposure of personal information.

Reputational damage is also a major concern. The misuse or public dissemination of private data can harm an individual's social image and relationships. In some cases, victims may face social isolation or discrimination as a result of cyber incidents.

Cybercrime is unique in its permanence and replicability. Once data is shared online, it can be copied and distributed indefinitely. This means that the

effects of cybercrime can persist long after the initial incident, prolonging the victim's distress.

Another challenge faced by victims is secondary victimization. When victims attempt to report cybercrime, they may encounter insensitive responses, bureaucratic delays, or lack of support from authorities. These negative experiences can discourage victims from pursuing justice.

Additionally, many victims blame themselves for the incident, especially in cases involving scams. This self-blame further reduces the likelihood of reporting.

Understanding cybercrime victimization is crucial for addressing non-reporting behaviour. By recognizing the various forms of harm and the challenges faced by victims, policymakers and law enforcement agencies can develop more effective support systems.

IV. CONCEPT OF NON-REPORTING BEHAVIOUR

Non-reporting behaviour refers to the decision of victims not to report crimes to law enforcement authorities. In the context of cybercrime, this phenomenon is particularly widespread and contributes significantly to the "dark figure of crime."

One of the primary reasons for non-reporting is psychological factors. Victims often feel ashamed, embarrassed, or guilty about the incident. For example, individuals who fall victim to online scams may fear being judged or ridiculed by others. Emotional responses such as denial and shock can also delay reporting.

Social and cultural factors play an important role. In many societies, victims may avoid reporting due to fear of stigma or damage to their reputation. This is especially true in cases involving cyber harassment or misuse of personal images. Family and peer pressure may also discourage victims from approaching authorities.

Institutional factors further contribute to non-reporting. Many victims perceive law enforcement agencies as inefficient or unresponsive. They may believe that reporting will not lead to any meaningful action or recovery of losses. Complex procedures and lack of technical expertise within institutions can also discourage reporting.

Technological complexity is another barrier. Cybercrime often involves technical processes that may be difficult for victims to understand. Collecting digital evidence and navigating reporting systems can be intimidating, particularly for individuals with limited digital literacy.

Additionally, some victims consider the loss to be minor and not worth the effort of reporting. Others may prefer to resolve the issue privately.

Non-reporting behaviour has serious implications. It distorts crime statistics, weakens policy-making, and allows offenders to continue their activities without accountability.

Addressing non-reporting requires a comprehensive approach that includes awareness campaigns, simplified reporting mechanisms, and improved institutional support. Encouraging victims to come forward is essential for strengthening the criminal justice system and reducing cybercrime.

V. THEORETICAL PERSPECTIVES

Understanding non-reporting behaviour in cybercrime victimization requires a strong theoretical foundation. Criminological theories provide insights into why victims choose not to report incidents despite experiencing harm. These theories help explain decision-making processes, social influences, and structural barriers that contribute to silence among victims.

One of the most relevant frameworks is Rational Choice Theory. This theory suggests that individuals make decisions based on a cost-benefit analysis. In the context of cybercrime, victims weigh the perceived benefits of reporting—such as justice, recovery of losses, or prevention of further harm—against the potential costs, including time, emotional stress, and lack of guaranteed outcomes. If victims believe that reporting will not result in meaningful action or recovery, they may decide that the effort is not worthwhile. This rational evaluation often leads to non-reporting, especially in cases involving minor financial loss or uncertainty about the offender's identity.

Another important perspective is Routine Activity Theory, which focuses on the conditions necessary for crime to occur. According to this theory, crime happens when three elements converge: a motivated offender, a suitable target, and the absence of a capable guardian. In cyberspace, the absence of guardianship can extend beyond prevention to include weak reporting systems. When victims perceive that there

are no effective authorities or systems to protect them or respond to their complaints, they may feel discouraged from reporting. Thus, weak institutional support contributes to both victimization and non-reporting.

Labelling Theory also plays a significant role in explaining non-reporting behaviour. This theory emphasizes the impact of social labels and stigma. Victims may fear being labelled as careless, irresponsible, or naïve, particularly in cases of online scams or fraud. This fear of negative judgement can lead to embarrassment and reluctance to disclose the incident. In societies where reputation is highly valued, this factor becomes even more influential.

Another relevant concept is Victim Precipitation Theory, which suggests that victims may perceive themselves as partially responsible for the crime. In cybercrime, victims often blame themselves for clicking on suspicious links, sharing personal information, or trusting unknown sources. This internalized blame reduces the likelihood of reporting, as victims may feel undeserving of support or fear being blamed by authorities.

These theoretical perspectives collectively highlight that non-reporting behaviour is not merely a personal choice but is influenced by a combination of psychological, social, and structural factors. Understanding these frameworks is essential for designing effective interventions that encourage reporting and support victims.

VI. IMPACT OF NON-REPORTING

Non-reporting behaviour in cybercrime has far-reaching consequences that extend beyond individual victims to affect society, law enforcement, and policy development. One of the most significant impacts is the distortion of crime statistics. When a large number of cybercrime incidents go unreported, official data fails to reflect the true extent of the problem. This "dark figure of crime" creates a misleading picture, making cybercrime appear less prevalent than it actually is.

Inaccurate statistics have serious implications for policy formulation. Governments and law enforcement agencies rely on data to allocate resources, design prevention strategies, and implement legal reforms. When data is incomplete, policies may be ineffective or misdirected. For example, insufficient reporting may lead to underfunding of cybercrime units or lack of investment in digital security infrastructure.

Another major impact is the continuation of criminal activity. When offenders are not reported, they are less likely to be identified, investigated, or punished. This lack of accountability allows cybercriminals to continue their activities and potentially target more victims. In some cases, offenders may become more confident due to the absence of consequences, leading to more sophisticated and widespread attacks.

Non-reporting also affects public trust in the criminal justice system. When victims choose not to report crimes, it often reflects a lack of confidence in authorities. This perception can create a cycle of distrust, where low reporting leads to limited action, which in turn reinforces the belief that reporting is ineffective. Over time, this weakens the relationship between citizens and law enforcement.

Additionally, non-reporting reduces the effectiveness of deterrence. The visibility of punishment plays a crucial role in discouraging criminal behaviour. When crimes are not reported, there is no visible consequence for offenders, which diminishes the deterrent effect of laws and regulations.

From a social perspective, non-reporting can lead to normalization of cybercrime. If victims remain silent, society may begin to accept cybercrime as an unavoidable part of digital life. This can reduce collective efforts to address the issue and undermine initiatives aimed at improving cybersecurity.

Therefore, addressing non-reporting behaviour is essential not only for supporting victims but also for strengthening the overall response to cybercrime. Encouraging reporting can improve data accuracy, enhance law enforcement effectiveness, and contribute to a safer digital environment.

VII. SOCIO-LEGAL FRAMEWORK IN INDIA

India has developed a socio-legal framework to address the growing challenge of cybercrime, combining legislative measures, institutional mechanisms, and technological initiatives. One of the key legal instruments is the Information Technology Act, 2000, which provides the foundation for regulating cyber activities and addressing offences such as hacking, identity theft, and data breaches.

Amendments to the Act have strengthened provisions related to cybersecurity and cyber terrorism.

In addition to legislation, the government has established specialized cybercrime cells within law enforcement agencies. These units are equipped to handle cyber-related offences and provide technical expertise in investigation. Furthermore, online reporting platforms, such as the National Cyber Crime Reporting Portal, have been introduced to simplify the complaint process and make it more accessible to the public.

Despite these developments, several challenges persist. One of the major issues is the lack of awareness among citizens about available legal remedies and reporting mechanisms. While urban populations may have better access to information and resources, rural areas often face limitations due to lower levels of digital literacy and infrastructure.

Another challenge is the complexity of legal procedures. Victims may find it difficult to navigate the reporting process, which can involve multiple steps, documentation, and technical requirements. This complexity can discourage individuals from filing complaints.

Institutional limitations also play a role. Law enforcement agencies may face constraints such as limited training, inadequate resources, and heavy workloads. These factors can affect the efficiency and responsiveness of cybercrime investigations, further reducing public confidence.

Privacy concerns are another significant barrier. Victims may fear that reporting a cybercrime could expose their personal information or lead to further victimization. Ensuring confidentiality and data protection is therefore crucial for encouraging reporting.

To strengthen the socio-legal framework, it is important to focus on awareness campaigns, capacity building, and technological innovation. Simplifying reporting procedures, providing victim support services, and enhancing transparency can help build trust in the system.

Overall, while India has made significant progress in addressing cybercrime, continuous efforts are needed to improve accessibility, efficiency, and public confidence in the legal framework.

VIII. RESEARCH METHODOLOGY AND FINDINGS

The study adopts a quantitative research design to examine non-reporting behaviour in cybercrime victimization. This approach is suitable for identifying patterns, trends, and relationships among variables. Data was collected through a structured questionnaire, which included both closed-ended and Likert-scale questions.

The sample consisted of approximately 100–250 respondents, including students, professionals, and other internet users. A stratified sampling technique was used to ensure representation across different demographic groups such as age, gender, and occupation. This method enhances the reliability and generalizability of the findings.

The questionnaire was divided into sections covering socio-demographic details, awareness of cybercrime, experiences of victimization, and reasons for non-reporting. Data analysis was conducted using descriptive statistics, including frequency distributions and percentages.

The findings reveal that a majority of respondents have a basic understanding of cybercrime. However, awareness of reporting mechanisms is relatively moderate, indicating a gap between knowledge of cybercrime and knowledge of how to respond to it.

One of the most significant findings is that privacy concerns are the primary reason for non-reporting. Many respondents expressed fear that their personal information could be exposed during the reporting process. This highlights the importance of ensuring confidentiality in cybercrime investigations.

Another key finding is the perception that reporting is ineffective. A considerable number of respondents believe that no meaningful action will be taken even if they report the incident. This reflects a lack of trust in institutional responses.

The study also identifies lack of digital literacy as a major barrier. Respondents indicated that limited knowledge of technology makes it difficult to report cybercrime. This is particularly relevant for older individuals and those in rural areas.

Additionally, the complexity of reporting procedures and fear of embarrassment were found to discourage reporting. Many respondents suggested that simplifying the reporting process and providing user-

friendly online platforms would encourage more victims to come forward.

Overall, the findings emphasize the need for awareness, education, and system improvements to address non-reporting behaviour effectively.

IX. CONCLUSION

The rapid growth of digital technology has transformed modern society, creating new opportunities as well as new risks. Cybercrime has emerged as a significant challenge, affecting individuals across different socio-economic backgrounds. Despite the increasing prevalence of cyber offences, non-reporting behaviour remains a critical issue that undermines efforts to combat cybercrime effectively.

This study highlights that non-reporting behaviour is influenced by a combination of psychological, social, cultural, and institutional factors. Victims often hesitate to report incidents due to fear of embarrassment, social stigma, privacy concerns, and lack of trust in authorities. Additionally, procedural complexities and limited digital literacy further discourage reporting.

The consequences of non-reporting are far-reaching. It leads to inaccurate crime statistics, weakens policy formulation, and allows offenders to operate without accountability. Moreover, it reduces public trust in the criminal justice system and diminishes the deterrent effect of laws.

Addressing non-reporting behaviour requires a comprehensive and multi-dimensional approach. Increasing public awareness about cybercrime and reporting mechanisms is essential. Educational initiatives and digital literacy programs can empower individuals to recognize and respond to cyber threats effectively.

Simplifying the reporting process is another crucial step. User-friendly online platforms and mobile applications can make it easier for victims to file complaints. Ensuring confidentiality and protecting victims' personal information can also help build trust and encourage reporting.

Strengthening law enforcement capabilities is equally important. Providing specialized training, improving infrastructure, and enhancing coordination among agencies can improve the efficiency of cybercrime investigations. Additionally, victim support services, including counselling and legal assistance, can help individuals overcome fear and hesitation.

Ultimately, encouraging victims to report cybercrime is not only a matter of individual justice but also a societal necessity. Bringing hidden crimes to light can improve data accuracy, enhance policy-making, and strengthen prevention strategies.

In conclusion, addressing non-reporting behaviour is essential for creating a safer digital environment. By fostering awareness, trust, and institutional responsiveness, society can move towards a more effective and inclusive approach to combating cybercrime.

REFERENCES

[1] Abdulai, Mohammed Awal. The Paradox of Cybercrime Risk and Internet Use in Canada: A Socio-Criminological Perspective. 2022.

[2] Anjum, Ubaid. Cybercrime in Pakistan: Detection and Punishment Mechanism. 2019.

[3] Asiamah, Aikins Amoako, and Hua Zhong. "Victims' Rational Decision: A Theoretical and Empirical Explanation of Dark Figures in Crime Statistics." 2022.

[4] Ballreich, Fabian Lucas, et al. "Encouraging Organizational Information Security Incident Reporting." Proceedings of EurAsEC 2023, 2023.

[5] Biedron, Scarlet Rosalie. Cybercrime in the Digital Age: How Big Data, Cryptocurrency, and Communication Networks Shape Cyber Offending, Cyber Security, and Law Enforcement. 2024.

[6] Bidgoli, Morvareed, and Jens Grossklags. "End User Cybercrime Reporting: What We Know and What We Can Do to Improve It." 2016.

[7] Buil-Gil, David, et al. "Cybercrime and Shifts in Opportunities During COVID-19: A Preliminary Analysis in the UK." 2021.

[8] Chalak, Ayman. Cyber-Crime in Online Videogames and Its Reporting by School-Aged Children. 2020.

[9] Cooper, Carolyn. "Financial Cybercrime and Older Adults: A Realist Review." Experimental Gerontology, 2021.

[10] Cross, Cassandra. "No Laughing Matter: Blaming the Victim of Online Fraud." 2015.

[11] ---. "Using Financial Intelligence to Target Online Fraud Victimization: Applying a Tertiary

Prevention Perspective." Criminal Justice Studies, 2016.
[12] ---. "Victims' Motivations for Reporting to the 'Fraud Justice Network.'" 2018.
[13] Cross, Cassandra, Kelly Richards, and Russell Smith. Improving Responses to Online Fraud Victims: An Examination of Reporting and Support. 2016.
[14] Curtis, Joanna, and Gavin Oxburgh. "Understanding Cybercrime in 'Real World' Policing and Law Enforcement." 2022.
[15] Dreißigacker, Arne, et al. "Online Hate Speech Victimization: Consequences for Victims' Feelings of Insecurity." 2024.