DIGITAL VICTIMIZATION IN INDIA: A LEGAL STUDY

Himalay Gaund, Research Scholar, Department of Law, School of Legal Studies, BBAU, Lucknow.

Introduction

The arrival of digital technology has transformed communication, business, education, and practically every area of contemporary life. India, experiencing rapid internet penetration and a flourishing digital ecosystem, has seen its very fabric change the way information flows and is consumed. Nevertheless, this digital revolution comes with its share of issues. With greater dependence on web-based technologies, a dark underbelly has resulted in the form of digital victimization through which victims are becoming easy prey for cybercrimes like cyberbullying, identity theft, online fraud, cyberstalking, and numerous other misuses of data. This article penetrates deep into the reality of digital victimization in India, its manifestations, current legal framework, enforcement challenges, and suggestions for future development.

India's digital journey started slowly but has taken a fast pace in the last two decades. The passage of the Information Technology (IT) Act in 2000 was a milestone moment that indicated the government's intention to regulate and protect the digital space. Through initiatives like Digital India, the country has seen a rapid growth in internet penetration, and digital platforms have become an integral part of daily life.[1]

But this expansion has also brought more digital crimes. With millions of Indians going online, the risk of cybercrimes has multiplied manifold. This expansion of digital activity, accompanied at times by limited digital knowledge and infrastructural issues, has placed the challenge of fighting digital victimization on the highest policy and law enforcement agenda.

Defining Digital Victimization

Digital victimization is any type of psychological, financial, or reputational damage that a person incurs as a consequence of digital or online behavior. While conventional crimes tend

[1] Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., Duan, Y., Dwivedi, R., Edwards, J., Eirug, A., Galanos, V., Ilavarasan, P. V., Janssen, M., Jones, P., Kar, A. K., Kizgin, H., Kronemann, B., Lal, B., Lucini, B., . . . Williams, M. D. (2019). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *57*, 101994. https://doi.org/10.1016/j.ijinfomgt.2019.08.002

to leave visible marks, digital crimes can be subtle and extensive. Victims can suffer long-term emotional trauma, financial loss, or even social exclusion as a result of cyber-attacks, fraud, or unauthorized sharing of personal information.[2]

The anonymity and transnationality of the internet create the perfect stage for perpetrators. Whether it is a sophisticated hacking attack or an ill-considered act of cyberbullying, the virtual space provides the tools and the means of cover for criminal enterprise. For a nation as large and multifaceted as India, the explosive expansion of digital spaces has opened up new channels for victimization, requiring a strong legal and technological response.[3]

Types of Digital Victimization in India

Digital victimization in India can be broadly categorized into several types. Each type poses unique challenges for legal authorities and requires specialized interventions:

1. **Cyberbullying and Harassment**

   Cyberbullying refers to the process of using digital media social media, messaging apps, or online forums to harass, humiliate, or intimidate people. The victims usually experience psychological distress, and as a result, suffer severe emotional and mental health consequences. Instances of cyberbullying are highly concerning among teenagers and youth, in which online harassment sometimes even results in fatal consequences.[4]

2. **Identity Theft**

   Identity theft is the most common type of online victimization. It takes place when an offender obtains unauthorized access to an individual's personal information, including bank account details, Aadhaar details, or other sensitive identifiers. The stolen identity can be used for financial fraud or further criminal activities in the victim's name.[5]

[2] Novak, A. (2016). *Defining identity and the changing scope of culture in the digital age*. IGI Global.

[3] Agustina, J. R. (2015). Understanding Cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology*, *9*(1), 35–54. https://doi.org/10.5281/zenodo.22239

[4] Leslie, R. S. (2020). *Handbook of Research on Cyberbullying and Online Harassment in the Workplace*. IGI Global.

[5] Ahmed, S. R. (2020). *Preventing Identity Crime: identity theft and identity fraud: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity Crime*. BRILL.

3. **Online Financial Fraud**

Online financial fraud encompasses a wide spectrum of fraudulent tactics like phishing scams, credit card scams, and electronic payment scams. Scammers use high-level methods of deception to get victims to reveal sensitive information. Financial consequences can be devastating, placing victims in extreme financial conditions and eroding trust within digital financial networks.[6]

4. **Cyberstalking**

Cyberstalking is defined as repeated, unwelcome online surveillance or contact which results in the victim feeling a sense of fear and distress. The stalker frequently employs numerous online resources in order to observe the victim's behavior, on occasion spilling over into off-line harassment. Not only does this type of victimization compromise personal privacy but also creates an ongoing feeling of vulnerability.

5. **Revenge Porn and Image-Based Abuse**

Revenge porn is the unauthorized dissemination of intimate images or footage, often in an attempt to humiliate or blackmail the victim. This cyber abuse can lead to crippling social and psychological repercussions. In spite of legal steps being taken, instances are still being reported, underlining the challenge of entirely eliminating this intrusive behavior.[7]

6. **Fake News and Online Defamation**

The advent of social media has also promoted the spread of disinformation and fake news. Online defamation where false information is circulated knowingly to ruin an individual's reputation has become a serious issue. Defamation victims tend to suffer long-term reputational damage, which impacts personal as well as professional life.[8]

[6] "Nawab, R. (2024). *Virtual Vipers: Unmasking the secrets behind online financial scams*. Blue Rose Publishers.

[7] Image-Based sexual abuse: A Study on the Causes and Consequences of Non-Consensual Nude Or Sexual Imagery. (2022). Routledge.

[8] Chakraborty, T., Shu, K., Bernard, H. R., Liu, H., & Akhtar, M. S. (2021). *Combating Online Hostile Posts in Regional Languages during Emergency Situation: First International Workshop, CONSTRAINT 2021, Collocated with AAAI 2021, Virtual Event, February 8, 2021, Revised Selected Papers*. Springer Nature.

7. **Hacking and Data Breaches**

   Hacking incidents and data breaches may result in the loss of sensitive organizational and personal information. The effects vary from financial losses to exposure of personal secrets, which can be used for blackmail or other criminal activities. The sophistication of cyber-attacks, combined with the dynamic nature of hacking methods, renders them a powerful challenge to law enforcement.[9]

The Legal Framework in India

India has established a multifaceted legal framework to address digital crimes. This framework includes specialized cyber laws, amendments to existing legal codes, and various judicial precedents that together create a comprehensive, though continually evolving, legal landscape.[10]

The Information Technology (IT) Act, 2000

The IT Act, 2000, forms the cornerstone of India's legal approach to digital crimes. Enacted to provide legal recognition for transactions carried out by electronic means, the act has evolved to address the challenges posed by cybercrimes. Key provisions include:

- **Section 66:** This section addresses offenses related to hacking and unauthorized access to computer systems. It serves as a deterrent to those who attempt to breach digital security.[11]

- **Section 66C:** Specifically targets identity theft by criminalizing the unauthorized use of another person's digital identity.[12]

- **Section 66D:** Focuses on cheating by impersonation, where fraudsters use digital means to deceive victims.[13]

- **Section 67:** Prohibits the publication or transmission of obscene material in electronic

[9] Davidoff, S. (2019). *Data breaches: Crisis and Opportunity*. Addison-Wesley Professional.

[10] Krishnaswamy, S., Sane, R., Shah, A., & Aithala, V. (2022). *Crime victimisation in India*. Springer Nature.

[11] Sharma, V. (2011). *Information Technology law and practice*. Universal Law Publishing.

[12] Manglik, R. (2024). *Information Technology Law: [9789369065097]*. EduGorilla Publication.

[13] Soni, M. (2024). *Security and Cyber Laws Digital defenders*.

form, thus safeguarding the moral and ethical standards of digital content.[14]

- **Sections 67A and 67B:** These provisions extend the protection to cases involving sexually explicit content and child pornography, ensuring that vulnerable populations are shielded from exploitation.[15]

While the IT Act provides robust mechanisms for addressing a range of cyber offenses, critics argue that its scope sometimes falls short in addressing newer forms of digital crimes. Furthermore, the act's rapid amendments have occasionally led to ambiguities that challenge consistent judicial interpretation.

Bharatiya Nyaya Sanhita (BNS)

- The Bharatiya Nyaya Sanhita (BNS), India's new penal code, addresses digital victimization by expanding the scope of offenses like forgery, extortion, and hate speech to include electronic communication, and by introducing provisions for cybercrime-related offenses.[16]

- **Section 78:** Addresses cyberstalking, providing legal recourse for victims of persistent digital harassment.

- **Sections 356:** These sections, originally aimed at defamation, have been extended to cover online defamation. They provide the legal foundation for prosecuting individuals who tarnish reputations through false digital claims.

- **Section 351(4):** Deals with criminal intimidation, including anonymous threats made through digital platforms.

- **Section 318:** Known for addressing fraud, this section is often invoked in cases of online financial scams and deceptive practices.

The incorporation of the IPC with contemporary digital issues accentuates the resilience of classic legal systems. But it also highlights the imperative for ongoing reforms to keep up with

[14] Manglik, R. (2024b). *Information Technology Law: [9789369065097]*. EduGorilla Publication.

[15] Soni, M. (2024). *Security and Cyber Laws Digital defenders*.

[16] Biswal, M. (2024). *New Criminal Laws Past and Present Bharatiya Nyaya Sanhita, 2023 with IPC 1860*. OrangeBooks Publication.

fast-changing technologies.[17]

The Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act was brought in to address sexual crimes against children, including those that are perpetrated in the digital space. With specific provisions that criminalize the exploitation and abuse of children in the digital space, the act is a landmark step in safeguarding one of the most vulnerable groups of the population. Where explicit digital content or online solicitation is involved, the POCSO Act is complemented by the IT Act to ensure a layered legal response.[18]

The Consumer Protection Act, 2019

With e-commerce and online transactions becoming a part of day-to-day life, the Consumer Protection Act, 2019, has been an important legal tool. The act is focused on issues like deceptive advertisements, scam online transactions, and bogus trade practices in the online environment. By giving rights to consumers and efficient grievance redressal procedures, the act reduces some of the ill effects of digital victimization in the context of business.[19]

Case Studies of Digital Victimization in India

A closer examination of specific case studies provides valuable insights into the multifaceted nature of digital victimization in India. These cases illustrate the diverse ways in which individuals and organizations have been affected, as well as the complexities involved in legal redress.[20]

Case Study 1: Cyberbullying and Its Long-Term Impact

In a much-publicized case in 2018, a young student in a metropolitan city went through acute cyberbullying after posting a personal video online. The out-of-context video was shared without permission and created extreme online abuse. The victim had anxiety, depression, and social isolation, and the legal fight that ensued pointed to the difficulty in getting immediate

[17] Biswal, M. (2024). *New Criminal Laws Past and Present Bharatiya Nyaya Sanhita, 2023 with IPC 1860*. OrangeBooks Publication.

[18] Singh, A., & Varma, P. (2025). *Child Sexual Abuse in India: A comprehensive treatise on POCSO*. Chyren Publication.

[19] Datey, V. (2020). *Overview of Consumer Protection Act, 2019*. Taxmann Publications Private Limited.

[20] Halder, D. (2021). *Cyber victimology: Decoding Cyber Crime Victimization*. Routledge.

judicial relief. Though the IT Act was finally enforced, the lateness in taking evidence and the challenge of tracking down the criminals added to the victim's torment.

Case Study 2: Identity Theft and Financial Fraud

Another high-profile case was that of a person whose online identity was hacked and used to make unauthorized financial transactions. The victim, who had been careful to protect personal data, found suspicious activity on bank accounts and online wallets. Although the authorities were informed promptly, the intricate nature of online trails and the cross-jurisdictional nature of the offense meant that the investigation took a long time. The subsequent prosecution under Section 66C of the IT Act and Section 420 of the IPC highlighted the significance of timely legal action and enhanced digital forensic techniques.[21]

Case Study 3: Revenge Porn and Image-Based Abuse

Revenge porn is still one of the most socially and emotionally harmful types of digital victimization. There has been a particular case where intimate photos were posted online without authorization as a form of revenge after a personal breakup. The victim not only endured humiliation and damage to reputation but also suffered the additional trauma of watching private moments become public pulp. Though legal provisions in the IT Act were invoked, the case revealed key loopholes in evidence gathering and the sluggish pace of judicial process in sensitive cases.[22]

Case Study 4: Online Fraud in the E-Commerce Sector

The exponential growth in India's e-commerce sector has been followed by an influx of cybercriminals targeting consumers using deceitful frauds. Phishing scams and counterfeit websites in various cases tricked naive shoppers into sharing their credit card and personal details. Not only resulted in monetary loss but also cultivated an all-round mistrust towards online marketplaces. The legal reaction, mainly under the Consumer Protection Act and the IT Act, has been plagued by jurisdictional issues and problems in tracing the origin of the spurious

[21] Halder, D. (2021). *Cyber victimology: Decoding Cyber Crime Victimization*. Routledge.

[22] Fido, D., & Harper, C. A. (2020). *Non-consensual image-based sexual offending: Bridging Legal and Psychological Perspectives*. Springer Nature.

operations.[23]

Challenges in Combating Digital Victimization

While India's legal framework provides a solid foundation for addressing digital crimes, several challenges remain in effectively combating digital victimization:

1. Jurisdictional Issues

One of the foremost challenges is the cross-border nature of many cybercrimes. Digital crimes rarely respect geographical boundaries, and perpetrators can operate from locations that fall outside the jurisdiction of Indian law enforcement. This poses significant obstacles to prosecution, as international cooperation and mutual legal assistance treaties become critical factors in bringing cybercriminals to justice.[24]

2. Limited Digital Literacy

Despite rapid technological advancement, digital literacy in India remains uneven. A significant portion of the population, particularly in rural and remote areas, lacks the necessary skills and awareness to protect themselves online. This digital divide not only makes individuals more vulnerable to cybercrimes but also hinders the reporting process, as many victims remain unaware of the legal remedies available to them.

3. Anonymity and Encryption

The very features that make digital platforms appealing—namely, ease of access and anonymity—also provide cover for criminals. Sophisticated encryption technologies and anonymizing tools allow perpetrators to hide their identities, making it exceedingly difficult for law enforcement agencies to trace and apprehend them. This challenge is compounded by the rapid pace at which technology evolves, often outstripping the capacity of legal frameworks to adapt.

[23] Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law And Safety*, *89*(2), 207–216. https://doi.org/10.32631/pb.2023.2.19

[24] Lahby, M., Pathan, A. K., & Maleh, Y. (2023). *Combatting Cyberbullying in Digital Media with Artificial Intelligence*. CRC Press.

4. Slow Judicial Processes

The judicial system in India, like in many other countries, is often criticized for its slow pace. Cybercrime cases require specialized knowledge, and delays in investigation and trial can exacerbate the victim's suffering. The need for digital forensic evidence and expert testimony further complicates the legal process, resulting in prolonged litigation that can undermine public confidence in the system.[25]

5. Insufficient Cyber Forensics Infrastructure

Effective investigation of digital crimes requires a robust infrastructure for cyber forensics. Currently, there is a noticeable shortage of trained professionals and state-of-the-art forensic laboratories in India. Without the necessary resources to accurately analyze digital evidence, many cases remain unresolved or are mishandled, leaving perpetrators free to commit further offenses.

6. Underreporting of Cybercrimes

Many victims of digital crimes choose not to report incidents due to fear of social stigma, embarrassment, or skepticism about the effectiveness of legal recourse. This underreporting creates a significant gap in data, making it challenging for policymakers and law enforcement to gauge the true extent of digital victimization and to allocate resources appropriately.[26]

The Role of Technology and Public-Private Partnerships

Combating digital victimization is best done by using a multifaceted response that extends beyond law enforcement efforts. The interaction of technology with the legal landscape is key to formulating good solutions.

Advancements in Cyber Forensics

Investment in cyber forensics infrastructure is crucial. Equipped with cutting-edge laboratories and well-trained experts, law enforcement can trace digital footprints more effectively and

[25] Lahby, M., Pathan, A. K., & Maleh, Y. (2023). *Combatting Cyberbullying in Digital Media with Artificial Intelligence*. CRC Press.

[26] Lahby, M., Pathan, A. K., & Maleh, Y. (2023). *Combatting Cyberbullying in Digital Media with Artificial Intelligence*. CRC Press.

collect admissible evidence. Upgrading forensic capacity will not only enhance the pace of investigations but also enhance the rate of success in prosecuting criminals.[27]

Public-Private Partnerships

A partnership between government institutions and private technology firms can build a stronger defense against cybercrime. Tech corporations have the knowledge and technological resources required to intercept, block, and track digital crimes. Through information sharing and collaboration, the two sectors can cooperate to develop stronger security measures and an efficient response system when problems arise.

Cybersecurity Awareness and Education

An important aspect in the minimization of digital victimization is the encouragement of digital literacy. Initiatives by the government, with involvement from private institutions and non-governmental organizations, need to be directed towards raising citizens' awareness on the best practices in cybersecurity. Such campaigns can enable the public to become aware of possible dangers, take preemptive action, and know the legal redress offered in the event of cybercrime.[28]

International Collaboration

Since digital crimes are borderless in character, international cooperation is imperative. India will have to cooperate in close association with other nations in order to sign treaties and cooperative mechanisms that allow for the speedy sharing of information and joint action against cybercriminals who work across national borders. International cooperation can address the jurisdictional hurdles over which digital crime investigations have historically groaned.[29]

Evolving Legal Reforms and Future Directions

The ever-changing nature of technology requires that the legal framework also change on a

[27] Harisha, A., Mishra, A., & Singh, C. (2023). *Advancements in cybercrime investigation and digital forensics*. CRC Press.

[28] Lahby, M., Pathan, A. K., & Maleh, Y. (2023). *Combatting Cyberbullying in Digital Media with Artificial Intelligence*. CRC Press.

[29] Ayodele, J. O. (2019). *Global Perspectives on Victimization Analysis and Prevention*. IGI Global.

regular basis. Various reforms are being contemplated and in different stages of implementation, with the objective of making the response to digital victimization in India more robust.

1. Comprehensive Cyber Laws

While the IT Act has been the core of India's cyber law framework, there is increasingly a consensus on the requirement for more robust legislation. Future legislation must address directly emerging issues like the abuse of artificial intelligence, deepfakes, and more advanced means of online manipulation. This would ensure that legal stipulations stay current and effective in the era of fast-changing technologies.[30]

2. Streamlined Judicial Processes

Judicial reforms to speed up cybercrime cases are a priority. There should be specialized cybercrime courts and expedited legal processes to cut down the lag time in case settlements. It not only benefits the cause of justice but also enhances public trust in the justice system. Quick settlement of cases would also act as a deterrent to leave prospective wrongdoers uneasy about committing digital crimes.

3. Strengthening Data Protection Laws

As the amount of digital data generated continues to grow, protecting data has become more important. Effective data protection legislation that outlines clearly the rights of individuals and the obligations of organizations can lower the risk of data breaches and unauthorized use. Such legislation should also include strong provisions for victims to obtain redress in instances of misuse of data.

4. Empowering Cyber Forensics and Investigation Units

Governments need to invest in constructing specialized cyber forensic units in police forces and judicial institutions. By using updated technology and training, these units can enhance their ability to deal with advanced cybercrimes. Improved forensic capabilities will play a

[30] Jariwala, M. (2023). *The Cyber Security Roadmap A comprehensive guide to cyber threats, cyber laws, and cyber security training for a safer digital world*. Mayur Jariwala.

crucial role in delivering justice to the perpetrators and in regaining public confidence in the system.[31]

5. Legal Support and Rehabilitation for Victims

Digital victimization tends to leave victims bearing emotional and economic scars. Creation of specialized helplines, legal aid clinics, and rehabilitation programs is important to assist victims through the judicial process and facilitate their recovery from the ordeal. A compassionate strategy, in conjunction with legal remedies, can remove the long-term effects of cybercrimes from individuals and society.[32]

Comparative Analysis: Lessons from Other Jurisdictions

As India further formulates legal responses to digital victimization, it is illuminating to examine how other nations have tackled comparable issues. Comparative examination offers important lessons on best practices and pitfalls to avoid.

The European Union's Approach

The EU has taken end-to-end data protection and cybersecurity steps, in particular, by the General Data Protection Regulation (GDPR). GDPR's rigorous standards of data management and heavy penalties for not adhering to them are an effective deterrent to data breaches and illegal digital practices. India can learn from the GDPR example and make its data protection legislation robust enough to make citizens and institutions accountable for online security.

The United States Legal Framework

The United States has a patchwork of federal and state legislation covering cybercrime. It has agencies like the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) operating in close coordination to investigate and counter cybercrimes. Although the U.S. system is supported by superior technology resources, it suffers from

[31] Harisha, A., Mishra, A., & Singh, C. (2023). *Advancements in cybercrime investigation and digital forensics*. CRC Press.

[32] Agarwal, S., Kayal, S., Pal, S., Hassan, S. T., J, A. M., C, B., Omeje, S. O., Oparaugo, B., Chukwuka, M. O., Naim, M. J., Ferdaous, J., Alam, I. S., Abdelhadi, A., Bhar, P., Chatterjee, M., Vaidya, A., Ghosh, S., Sewa, N., Otuya-Asohro, E. O., . . . Aman, M. (2024). *Emergence of Social Media: Shaping the digital discourse of the next generation*. Sayak Pal.

conflicting jurisdictions and bureaucratic resistance. Nevertheless, the U.S. experience highlights the necessity of having specialized task forces and inter-agency coordination for countering cybercrime.

Adopting Best Global Practices

India's policy makers could also learn from observing international practices in a detailed and cautious manner. Adopting efficient models like speedy cybercrime courts and digital forensic investigation units would go a long way in India's capacity for combating digital victimization. Multilateral cooperation on research and transfer of technology from international agencies would also translate to improved prevention as well as prosecution of cybercrime.

Recommendations for a Safer Digital Future

On the basis of the above analysis, some important policy recommendations follow for policymakers, law enforcement organizations, and society as a whole:

1. Update and Enrich Cyber Laws: Legislation in the future must cover coming digital challenges like AI-based cyberattacks, deepfakes, and changing social media trends. Well-defined, unambiguous laws that evolve with technological advancements are crucial.

2. Invest in Cyber Forensics: Enhancing investment in cyber forensic labs, training of specialized staff, and the implementation of the latest technologies will enhance the speed and efficiency of digital crime investigations.

3. Strengthen International Collaboration: Cybercrime is a global issue. India must establish closer relationships with international law enforcement agencies and engage in global cybersecurity forums to exchange intelligence and best practices.

4. Encourage digital literacy: Countrywide campaigns for citizens to learn about digital security measures, online safety practices, and legal rights are essential. Particular emphasis should be placed on vulnerable groups in rural and far-flung areas.

5. Establish Victim Support Systems: Organizing specific centers providing legal guidance, psychological counseling, and financial advice can assist digital crime victims in recovering and being rehabilitated back into society.

6. Develop Specialized Cybercrime Units: The establishment of specialized cybercrime cells with the responsibility of investigating cybercrimes will eliminate the lag in case resolution and ensure that offenders are brought to justice promptly.

7. Use Technology for Prevention: Partnering with technology firms to create sophisticated monitoring and threat detection systems can prevent digital crimes from happening in the first place. Early warning systems and AI-based analytics can be important tools in detecting potential threats.

Conclusion

Digital victimization in India is a multifaceted challenge that intersects technology, law, and society. The ever-increasing sophistication of cybercrimes and the quickening pace of digital platforms require a solid, adaptive legal system and concerted cooperation between the public and private sectors. While India has achieved much with the IT Act, IPC modifications, and enabling laws such as the POCSO and Consumer Protection Acts, the way forward entails ongoing innovation and reform.

To really lock in India's digital future, there has to be a collective effort to modernize legal frameworks, improve investigative capabilities, and sensitize the public to cybersecurity practices. The lessons learned from global best practices and the experiences of other jurisdictions can be invaluable guides in this effort. As online platforms continue to mold the social fabric, a holistic, flexible, and visionary legal response will be necessary in protecting citizens from the various dangers of digital victimization.

Finally, a more secure cyber environment in India is not solely the state's responsibility—it needs the active involvement of all stakeholders, ranging from government institutions to the judiciary, private enterprises, and even citizens themselves. Only with a collaborative, pro-active effort can India aspire to stem the tide of digital crime and see to it that the dividends of digital transformation are not negated by the threat of cyber victimization.

In summary, though the development of digital technology presents enormous opportunities, it also requires strict legal examination and technological readiness. Upgrading legal provisions continuously, along with improved cyber forensics and global cooperation, can enable India to ride out the threats of digital victimization and establish a strong digital future. With continued efforts, a balance can be achieved between promoting digital innovation and safeguarding people from the negative aspects of the digital revolution.