RISE OF CYBERCRIME IN INDIA: LEGAL GAPS AND ENFORCEMENT CHALLENGES IN THE DOMAIN OF INDIAN LAW

Sakshi Singh, Amity Law School, Noida

ABSTRACT

In the last decade, India has witnessed an unprecedented surge in digital activity online banking, social media use, e-commerce, and virtual education have become everyday norms. However, this digital expansion has come at a cost. Cybercrime in India has grown alarmingly, affecting individuals, businesses, and government systems alike. From phishing scams that rob unsuspecting citizens of their savings, to large-scale ransomware attacks major corporations, cyber threats have taken a serious toll on the nation's safety and trust in digital platforms.

This research aims to provide a grounded, realistic view of the current state of cybercrime in India. It explores both the nature and growth of cybercrimes such as hacking, data breaches, identity theft, cyberstalking, and financial fraud and critically analyses the legal framework designed to combat them. The study focuses on India's key laws, primarily the Information Technology Act, 2000 and relevant provisions of the Indian Penal Code, and assesses whether they are capable of handling 21st-century digital threats.

Law enforcement faces its own set of challenges. Cyber police cells in many Indian states lack trained personnel, modern digital tools, and even basic infrastructure. Officers often struggle with identifying and preserving digital evidence, which weakens the prosecution's case in court. To make matters worse, many victims, especially women, choose not to report incidents like cyberbullying or online sexual harassment due to fear, shame, or lack of awareness.

This paper also considers the role of the judiciary through key cases such as *Shreya Singhal v. Union of India*, which struck down the controversial Section 66A of the IT Act for curbing free speech, and *Avnish Bajaj v. State*, which addressed intermediary liability. These rulings reflect a slow but evolving judicial understanding of cyber issues.

Keywords: Cyberspace, Crime against Women and Children, Data Protection,

Introduction

Over the past decade, India has undergone a remarkable digital transformation. With widespread use of smartphones, internet penetration in rural and urban areas, and ambitious government campaigns like Digital India, citizens today are more connected than ever before. From making online payments to accessing government services, the digital sphere has become a crucial part of everyday life. But alongside these benefits lies a growing threat cybercrime. As more Indians go online, the chances of falling victim to cyberattacks have multiplied, and unfortunately, our laws and law enforcement are struggling to keep up with this fast-moving danger.[1]

Cybercrimes in India are no longer limited to tech-savvy hackers in dark rooms. They involve a wide range of offences: identity thefts, phishing scams, ransomware attacks, online sexual harassment, and even cyberterrorism. According to the National Crime Records Bureau (NCRB), cybercrime cases have seen a sharp year-on-year rise, with over 65,000 cases reported in 2023 alone—a number that likely represents just the tip of the iceberg due to underreporting and lack of awareness.

What makes cybercrime particularly dangerous is that it is borderless, faceless, and rapidly evolving. One can be sitting in Delhi and be defrauded by someone operating anonymously from another continent. Unfortunately, India's legal framework mainly governed by the Information Technology Act, 2000 and selected provisions from the Indian Penal Code, 1860 is not always equipped to address the complexities of modern digital offences.

Further compounding the issue are serious enforcement challenges. Police stations in many regions still lack dedicated cyber cells, and officers are often not trained in digital forensics. Victims frequently encounter delays, and even when a case is filed, it may take years to reach a conclusion in court. Meanwhile, offenders continue exploiting legal loopholes and jurisdictional grey areas with ease.

This paper aims to unpack the rise of cybercrime in India, analyze the gaps in the legal framework, and assess the challenges faced by enforcement agencies. By exploring real cases,

[1] National Crime Records Bureau (NCRB), *Crime in India Report 2023*, Ministry of Home Affairs, Government of India.

relevant laws, and global best practices, the goal is to suggest actionable reforms that can make India's cyberspace more secure for all.[2]

LITERATURE REVIEW

The growing cyberthreats in India and the necessary defences against them have been the subject of numerous studies by academics and researchers. Kshatriya (2019) examined India's quick digital adoption. Payment systems and discovered that whereas digital transactions improve financial inclusion, they can lead to cybersecurity concerns. The study demonstrated how cybercriminals perpetrate financial fraud by taking advantage of lax authentication procedures and vulnerabilities in digital infrastructure[3]. The function of artificial intelligence (AI) in preventing cybercrime was covered by Bansal & Arora (2021). Their study looked at how AI-powered security systems can automate threat responses, anticipate cyberattacks, and identify anomalous network activity. They determined that while AI-driven cybersecurity solutions greatly enhance threat detection capabilities, ongoing development is necessary to combat changing cyberthreats.

An extensive investigation into India's cyber laws and how well they work to combat cybercrimes was carried out by Sharma etc. in 2022 [4]. Their conclusions revealed that although the Information Technology Act of 2000 establishes a legal framework, law enforcement authorities' lack of awareness and insufficient resources make it difficult to implement cyber laws. To discourage cybercriminals, the report suggested enacting stricter punishments and more robust regulatory frameworks[5] . The psychological effects of cybercrimes on victims were the main topic of Gupta & Malhotra (2023). According to their research, identity theft and other cybercrimes. Financial fraud, online harassment, and theft cause a great deal of emotional pain and erode public confidence in digital networks[6]. In order to assist victims in overcoming the repercussions of cybercrimes, they recommended the necessity of psychological therapy services and awareness programs. Verma (2023) investigated the suitability of international cyber security best practices for India. His study recommended that

[2] Information Technology Act, 2000; Indian Penal Code, 1860.
[3] Rajeev Kshatriya, *Digital Transactions and Cybersecurity in India: Financial Inclusion at Risk*, 7 J. Digit. Econ. (2019).
[4] Mehak Bansal & Shreya Arora, *AI-Driven Cybersecurity Systems: A Boon or Bane?*, 9 Indian J. Cyber L. & Tech. (2021).
[5] Ravi Sharma et al., *Effectiveness of Cyber Laws in India: An Empirical Review*, 12 L.J. India 65 (2022).
[6] Richa Gupta & Aakash Malhotra, *Psychological Implications of Cybercrime on Indian Victims*, 5 Ind. J. Cyber Psychol. 4 (2023).

India follow the best cyber-secure countries, including the United States, by implementing a multi-layered cybersecurity strategy [7] . Estonia and the United States. In order to create a robust cyber ecosystem, he underlined the significance of rigorous data protection regulations, cyber education initiatives, and public-private partnerships. Together, these studies show that cyberthreats in India are complex and call for a mix of technological, regulatory, and awareness-raising measures to lessen their effects. India has made great strides to fortify its cyber security system, but ongoing work is required to keep up with new threats.

OBJECTIVE OF THE RESEARCH

This study will lead to a better understanding of the legal framework for cybercrime in India. Some legal, regulatory and procedural issues in prosecuting or defending against criminal acts will be examined.

- Assess the adequacy of existing cybersecurity architecture and policies.
- Critically analyze the trends and patterns of cybercrime in India.
- Assess the legal framework against cybercrime in India.
- Provide recommendations to reduce cybercrime

Background

India's rapid digital transformation has brought it to the forefront of global innovation in information technology and digital services. However, with this advancement comes a parallel rise in cyber threats, including identity theft, ransomware attacks, financial fraud, and large-scale data breaches. As digital tools become increasingly embedded in everyday life from Unified Payments Interface (UPI) transactions to accessing e-governance services and online commerce the nation finds itself more exposed to cyber vulnerabilities[8].

With over 800 million internet users, India now represents one of the largest and fastest-growing digital user bases in the world. This surge in connectivity has simultaneously made

[7] Nikhil Verma, *Global Best Practices in Cybersecurity: Lessons for India from Estonia and the USA*, 10 J. Sec. & Cyber 99 (2023).
[8] Press Information Bureau, *Digital India Programme*, Ministry of Electronics and Information Technology (2023), https://pib.gov.in.

the country a prime target for cybercriminals who exploit digital systems through sophisticated methods such as phishing, sextortion, and ransomware. Critical sectors such as banking, healthcare, and education have faced attacks that not only compromise sensitive information but also threaten public safety[9].

The onset of the COVID-19 pandemic further accelerated the shift to digital platforms. With more individuals working remotely and depending on personal networks, security protocols became more fragile, creating fertile ground for cybercrime. According to data from the National Crime Records Bureau (NCRB), more than 65,000 cybercrime cases were reported in India in 2023 a figure that likely underrepresents the actual scale of the problem due to underreporting, lack of awareness, and fear of reputational damage[10].

Despite the alarming rise in cyber threats, India's legal framework remains insufficiently equipped to handle the complexity and volume of such crimes. The Information Technology Act, 2000, remains the principal legislation governing cyber offences, but its provisions were crafted during a period when the nature and scope of cybercrime were far more limited. Today, emerging technologies like artificial intelligence, blockchain, cryptocurrency, and deepfake software introduce legal challenges that the IT Act was never designed to address. Furthermore, the absence of a robust and comprehensive data protection law leaves citizens' personal data susceptible to misuse not just by malicious actors, but also by corporations operating without adequate oversight.[11]

Impact of Cyber Crime on Individuals and Society

Effects on Businesses: Cybercrime poses serious risks to e-commerce companies, which handle enormous client records in digital formats. Businesses must put strong security measures in place, such as encrypting financial data, to safeguard sensitive data[12]. If they don't, hackers may be able to access client data without authorization by taking advantage of security flaws.

[9] Telecom Regulatory Authority of India (TRAI), *Monthly Performance Indicators Report – December 2023*, https://trai.gov.in.
[10] National Crime Records Bureau, *Crime in India 2023 – Cyber Crimes*, Ministry of Home Affairs (2024), https://ncrb.gov.in.
[11] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[12] Ananya Singh, *Data Breach Risks in Indian E-Commerce: A Cybersecurity Perspective*, 14 J. Cyber L. & Pol'y 22, 25–28 (2022).

Effects on Infrastructure: Critical national infrastructures including electricity grids, hospital networks, and air traffic control systems are frequently the target of cybercriminals, including cyberterrorists. The potential threats of cyberattacks increase dramatically with a nation's technical advancements. A breach in these areas has the potential to seriously harm the economy, jeopardize public safety, and interrupt essential services[13].

Effects on Individuals: People are also directly impacted by cybercrime, particularly when it comes to crimes like identity theft and online blackmail. If their demands are not satisfied, cybercriminals may threaten to reveal private, sensitive, or even fake information. Such encounters can result in a loss of privacy, long-term psychological repercussions, and extreme emotional suffering. These are a few of the noteworthy consequences linked to cybercrimes, which affect India extensively. These crimes are widespread throughout the country and have an impact on both private citizens and governmental organizations[14].

CYBERSPACE: AN ANALYSIS

The National Cyber Security Policy of 2013 describes cyberspace as a dynamic and interconnected environment shaped by the interaction of people, software, and services, all of which are supported by a global network of Information and Communication Technology (ICT) devices and systems[15]. This concept of cyberspace began to evolve during the 1990s, especially with the rapid rise of the internet. Today, it represents more than just a communication tool it has become a digital environment where people engage in activities like chatting, playing games, sharing ideas, and accessing services and information through websites and applications.

Cyberspace is now an essential part of everyday life. It acts as a platform for intellectual debates, political discussions, business transactions, and social interaction. In simple terms, it connects computers and people across the globe[16]. The Merriam-Webster Dictionary defines cyberspace as:

---

[13] S. R. Das & Neha Chopra, *Cybersecurity and Critical Infrastructure in India: An Emerging Threat Landscape*, 18 Nat'l L.J. India 44, 47–49 (2023).
[14] Pooja Sharma, *Emotional and Legal Impact of Online Blackmail on Victims in India*, 6 Indian J. Victimology 77, 79–83 (2023).
[15] Ministry of Commc'n & Info. Tech., Gov't of India, *National Cyber Security Policy 2013* (July 2, 2013), available at https://www.cert-in.org.in.
[16] Cyberspace, Merriam-Webster Dictionary, https://www.merriam-webster.com/dictionary/cyberspace (last visited July 17, 2025).

"the online world of computer networks, especially the Internet," reinforcing its importance in modern communication.

Interestingly, cyberspace shares certain features with the physical world, such as place, size, distance, and route. But at the same time, it operates very differently. Unlike physical space, cyberspace has no fixed borders information can travel instantly from one part of the world to another, making it both powerful and unpredictable. In today's strategic and military context, cyberspace is now considered the fifth domain of warfare, following land, sea, air, and outer space. Countries like the United States and members of NATO have already recognized it officially[17]. The reason is simple: cyberattacks can come from anywhere and target anyone, regardless of geographic boundaries. Whether it's military, government, or civilian space, cyberspace has made national and international security more complex than ever before.

ISSUES AND CHALLENGES IN THE CYBERWORLD

In the modern era, cyberspace has emerged as the fifth domain of national security, alongside land, air, sea, and space. Between January 2017 and January 2018, over 22,000 Indian websites were hacked, including more than 100 official government portals[18]. This alarming number reflects the growing sophistication of cybercriminals, who continuously evolve their tools and techniques. As India pushes ahead with its *Digital India* mission, the risk to online safety and privacy becomes even more serious. With the Right to Privacy now recognized as a fundamental right by the Supreme Court in *Justice K.S. Putt swamy v. Union of India (2017)*, protecting digital information is no longer optional it's a constitutional mandate[19]. However, India's cyber defense system still has significant gaps. There are no formal bug-reporting mechanisms, many sectors lack clear cybersecurity policies, and the country is yet to develop a robust cyberwarfare protection strategy[20]. Above all, there is a pressing need for a strong legal and regulatory framework that can respond swiftly to emerging threats. From identity theft and financial scams to cyberbullying and misinformation, the range of cybercrimes has widened.

[17] Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 Colum. J. Transnat'l L. 609, 613–15 (2018).
[18] Press Trust of India, *Over 22,000 Indian Websites Hacked Between Jan 2017-Jan 2018: Govt*, Hindustan Times (Apr. 4, 2018), https://www.hindustantimes.com.
[19] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[20] Pavan Duggal, *Cyber Warfare and National Security in India: Gaps in the Legal Regime*, 25 Indian J. L. & Tech. 37–39 (2022).

This situation is made worse by outdated laws and weak enforcement, which fail to keep pace with the rapidly evolving digital landscape [21].

Moreover, privacy violations have become common due to the misuse of personal data, often shared or sold without the user's consent. Vulnerable groups such as women, children, and the elderly face higher risks of exploitation due to the digital divide and lack of awareness. The absence of strict laws to address modern issues like deepfake technology, child pornography, and intellectual property theft only worsens the situation[22]. The COVID-19 pandemic further highlighted these issues. In the name of public safety, digital surveillance and tracking apps were deployed, raising concerns about the erosion of personal freedoms and data security[23].

To secure its digital future, India must strengthen its legal system, improve cybersecurity infrastructure, spread digital literacy, and build global partnerships to tackle cross-border cybercrimes. A proactive and inclusive approach is essential to ensure that technology empowers citizens without compromising their rights and freedoms.

Jurisdictional Challenges in Cyberspace

Jurisdiction poses a major legal hurdle in effectively addressing cybercrime, especially due to the borderless nature of the internet. In many cases, cybercriminals, their victims, and crucial digital evidence are all spread across different countries. This disrupts the traditional model of territorial jurisdiction, which is typically based on physical locations. Because data can move globally in seconds, determining which country has the legal authority to investigate or prosecute becomes highly complex.

This lack of physical boundaries leads to conflicts between domestic laws, international legal uncertainties, and delays in investigation or prosecution. It becomes especially difficult to obtain digital evidence, enforce court orders, or extradite cybercriminals when multiple jurisdictions are involved. As Ryngaert observes, "the absence of coherent cross-border enforcement mechanisms significantly limits international cooperation in cybercrime cases[24]."

[21] Aparna Vishwanathan, *The Information Technology Act: A Critical Appraisal of India's Cyber Law Framework*, 17 Nat'l L. Sch. India Rev. 89, 91–94 (2021).
[22] Richa Bhargava & S. Iyer, *Gender and Digital Vulnerability: Risks of Cybercrime Against Women and Seniors in India*, 13 J. Info. Sec. Stud. 58, 60–63 (2023).
[23] Anjali Mehra, *COVID-19 and the Rise of Digital Surveillance in India*, 45 Econ. & Pol. Wkly. 76, 78–80 (2021).
[24] Cedric Ryngaert, *Jurisdiction in International Law* 141 (2d ed. 2015).

These jurisdictional limitations are clearly seen in legal disputes arising from online business transactions**.** Courts have had to reinterpret existing contract and tort laws to handle digital transactions conducted across borders[25].

For example, in *Impresario Entertainment & Hospitality Pvt. Ltd. v. S&D Hospitality*, the Delhi High Court held that mere booking or placing an order online does not establish jurisdiction. The court ruled that a contract is not formed at the point of ordering but at the location where acceptance and confirmation of the transaction take place.

Similarly, in the landmark case of *Renaissance Hotel Holdings, Inc. v. B. Vijaya Sai*, the court declined to hear a suit based solely on an online hotel booking made abroad**,** emphasizing that virtual presence alone is insufficient to confer territorial jurisdiction in India[26] .These rulings reflect a growing judicial trend of critically evaluating online actions in light of physical legal standards.

Legal Mechanisms for Protecting Digital Security in India

India's approach to digital security is steadily evolving, guided by a combination of laws, policy initiatives, and institutional frameworks. At the heart of this framework is the Information Technology Act, 2000, which serves as the primary legislation dealing with cybercrime, data protection, and digital communications. This Act is supported by various rules and sector-specific guidelines that help enforce cybersecurity protocols and tackle offences in the online space[27].

With the rising threat of cyberattacks and increasing digital dependency, the National Cyber Security Policy 2023 has been introduced to provide a more coordinated and strategic approach to cybersecurity. It focuses on strengthening digital infrastructure, promoting secure digital practices, and fostering a cyber-resilient environment across public and private sectors[28].

In a major leap towards personal data protection, the Digital Personal Data Protection Act, 2023

[25] *Impresario Ent. & Hospitality Pvt. Ltd. v. S&D Hospitality*, 2021 SCC Online Del 3223.
[26] *Renaissance Hotel Holdings, Inc. v. B. Vijaya Sai*, (2018) 253 DLT 680 (Del. HC).
[27] Information Technology Act, No. 21 of 2000, INDIA CODE (2000); Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).
[28] Ministry of Electronics & Information Technology, National Cyber Security Policy 2023 (India), available at https://www.meity.gov.in.

(DPDP Act) was introduced. This legislation establishes a structured framework for the collection, storage, and processing of personal data. It also grants individuals rights over their personal information and imposes obligations on entities handling such data, making data privacy a core legal right[29].

India's cybersecurity infrastructure also involves several key authorities:

- **Ministry of Home Affairs** – oversees cybercrime enforcement through dedicated cybercrime wings[30].
- **Ministry of Electronics and Information Technology (MeitY)** – responsible for framing digital policies and promoting cyber awareness[31].
- **Indian Cyber Crime Co-ordination Centre (I4C)** a national-level platform for tackling cybercrime through capacity building and investigation support[32].
- **CERT-In (Indian Computer Emergency Response Team)** acts as the national nodal agency for responding to cybersecurity threats[33].
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** protects systems and networks vital to national security and public safety[34].

Recognizing the need to address cybercrime more directly, India's criminal law has also undergone reforms. The Bhartiya Nyaya Sanhita, 2023 (BNS) includes specific provisions to handle digital offences. Sections such as:

- **Section 196 and 197**- deal with hate speech, especially through social media or digital platforms.

[29] Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
[30] Ministry of Home Affairs, Cyber Crime Prevention against Women and Children Scheme (India), available at https://www.mha.gov.in.
[31] Ministry of Electronics & Information Technology, available at https://www.meity.gov.in.
[32] Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs (India), available at https://cybercrime.gov.in.
[33] Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology, available at https://www.cert-in.org.in.
[34] National Critical Information Infrastructure Protection Centre (NCIIPC), available at https://www.nciipc.gov.in.

- **Section 353** – targets misinformation that may disturb public peace.
- **Section 294** – broadens the definition of obscene content to include digital material like videos or messages[35].

These updates reflect a stronger focus on regulating online behavior and tackling emerging threats in the digital world.

Additionally, the Bharatiya Sakshya Adhiniyam, 2023 (BSA) strengthens the evidentiary value of digital documents. Notably:

- **Section 57** recognizes electronic records like emails, texts, and social media posts as **primary evidence**, enhancing the speed and credibility of trials involving digital content.
- **Section 63** introduces safeguards and standards for the admissibility of such evidence, ensuring it meets technical and legal scrutiny before it can be used in court[36].

Cyber Child Pornography and the Need for Regulation

The rise of cyber child pornography is one of the darkest outcomes of the internet age. The digital world meant to connect and empower has sadly become a platform for some of the worst forms of exploitation[37]. Offenders take advantage of encrypted apps, dark web forums, and even everyday social media platforms to create, share, and view harmful content involving minors. What makes this even more horrifying is that these materials don't just harm children once; the trauma continues every time the content is viewed or circulated again, robbing victims of their dignity and privacy for years to come.

In India, the Protection of Children from Sexual Offences Act, 2012 (POCSO) has been a significant legal step in addressing child sexual abuse. It criminalizes the use of children in pornographic acts and provides child-friendly procedures during trials. However, despite this legal backing, our laws are still catching up with how quickly these crimes are evolving online.

[35] Bharatiya Nyaya Sanhita, No. 45 of 2023, 196, 197, 294, 353, INDIA CODE (2023).
[36] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, 57, 63, INDIA CODE (2023).
[37] ECPAT International, *Child Protection in the Digital Age: National Responses to Online Child Sexual Exploitation* (2018), https://www.ecpat.org/wp-content/uploads/2021/04/2021_Global-Policy-Paper_DigitalAge.pdf.

Many offenders are based in other countries, and with limited global cooperation and differing cyber laws, it becomes hard to catch and punish them. Meanwhile, platforms hosting this content often act slowly or lack strong safeguards altogether.[38]

Solving this issue requires a combination of strict laws, faster enforcement, and better cooperation—both domestically and internationally. Tech companies must play a bigger role by installing stronger monitoring systems and reporting suspicious content quickly. International treaties, like the Budapest Convention on Cybercrime, can help countries work together, share data, and bring criminals to justice regardless of where they operate from[39].

As expert Alisdair Gillespie points out, this fight isn't just about punishing crimes after they happen it's about prevention, international support, and proper regulation. Protecting children online must be treated as a serious human rights priority. Only with global teamwork and strong laws can we ensure that the internet is a safe place for every child, not a threat to their safety[40].

The Overlooked Problem of Child Erotica: A Hidden Danger

While much of the discourse surrounding online child exploitation focuses on overt forms of abuse and explicit content, there exists a far more subtle yet equally disturbing problem child erotica. This term refers to images and representations of children in sexually suggestive poses, often presented under the guise of artistic expression or "innocent photography[41]." These images are not always overtly pornographic but are crafted in a way that deliberately sexualizes children, thus blurring the lines between art and exploitation.

Websites and platforms that distribute such content often label it as "posing pictures" or "soft child pornography," cloaking their true nature with sanitized language. They argue for creative freedom, portraying these visuals as harmless or even beautiful depictions of childhood. However, this normalization and glamorization of exploitative imagery serve only to desensitize viewers and perpetuate a dangerous culture that commodifies children's bodies.

[38] Protection of Children from Sexual Offences Act, No. 32 of 2012, 13, INDIA CODE (2012).
[39] UNICEF, *Legal and Policy Analysis of Online Child Sexual Exploitation and Abuse in South Asia* (2021), https://www.unicef.org/rosa/reports/legal-analysis-online-child-sexual-exploitatio
[40] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention), available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.
[41] Tanya S. L. Lee, *Child Erotica and the Limits of Free Speech: A Comparative Analysis*, 19 Hastings Women's L.J. , 128–30 (2008).

[42]Such content can act as a gateway for individuals with predatory tendencies and fosters communities that validate and encourage exploitative behavior.

The internet's provides a significant advantage to offenders, who use encrypted platforms, fake identities, and closed groups to share, discuss, and trade such content. As Nirvan et al. (2023) highlight, offenders often use this veil of anonymity to initiate contact with minors, engage in online grooming, and slowly manipulate them into increasingly exploitative situations. Grooming can involve flattering, building emotional connections, or offering gifts eventually leading to explicit interactions or offline abuse. Unfortunately, such cases are frequently underreported and under-investigated, as the content may not always meet the legal threshold for child pornography in many jurisdictions.

The covert nature of child erotica makes it especially dangerous not just because of its psychological impact on victims, but because it often slips through the cracks of legal enforcement.

While existing laws, including India's Protection of Children from Sexual Offences (POCSO) Act, criminalize child pornography, they may lack the clarity or reach needed to effectively regulate non-explicit exploitative imagery[43]. Additionally, social media platforms and file-sharing websites often do not act swiftly enough to flag and remove such content, citing ambiguous content guidelines or relying heavily on user reports.

To address this neglected threat, both legal reform and social awareness are critical. Laws need to evolve to include "non-explicit but exploitative content", and judicial systems must be trained to distinguish between legitimate artistic work and material that facilitates child exploitation. Moreover, tech companies should develop AI-based filters capable of identifying patterns of child erotica and blocking its dissemination. Public awareness campaigns and education must also play a role in recognizing how harmful such "soft" content truly is.

Electronic Violence Against Women: A Growing Threat in the Digital Age

The digital age has revolutionized communication and connectivity, but it has also opened new avenues for gender-based violence, especially targeting women. Online platforms, meant to

[42] Ethel Quayle & Max Taylor, *Child Pornography and the Internet: Perpetuating a Cycle of Abuse*, 18 Deviant Behavior 331, 333–34 (1997).
[43] Protection of Children from Sexual Offences Act, No. 32 of 2012, 13–15, INDIA CODE (2012).

empower and connect individuals, are increasingly being misused to harass, exploit, and threaten women[44]. Crimes like cyberstalking, online defamation, impersonation, cyberbullying, voyeurism, email spoofing, and the non-consensual sharing of intimate content have become alarmingly frequent. Women find themselves at the center of these online attacks, often facing deeply personal and psychologically scarring experiences, which are facilitated by the anonymity and reach of the internet.

One of the most distressing forms of digital violence is revenge pornography the malicious act of sharing private and intimate content without consent, usually by ex-partners aiming to cause humiliation or emotional damage.[45] Victims are often blackmailed, harassed, or threatened, with their personal content being shared on social media or pornographic websites. This not only shatters their reputation but also leads to immense mental distress, social isolation, and in extreme cases, even suicide.

According to a 2018 study by Freedom House, 58% of surveyed women reported experiencing some form of cyber violence, indicating how widespread and systemic the problem is[46]. Unfortunately, despite these staggering numbers, most victims remain silent, fearing social stigma, reputational damage, or further harassment. Additionally, the anonymous nature of the internet makes it difficult for law enforcement agencies to trace offenders or gather admissible digital evidence.

Legal remedies do exist in India under the Information Technology Act, 2000 and the Indian Penal Code, but enforcement remains weak. Provisions specifically addressing online harassment, identity theft, voyeurism, and cyber defamation are in place, yet delays in investigation, low conviction rates, and limited cyber forensics support continue to act as major hurdles. Furthermore, many police officers lack adequate training in handling such sensitive and tech-oriented cases, leading to further victim frustration[47].

Addressing this issue requires a multi-pronged approach stricter implementation of cyber laws,

[44] Barkha Shukla, *Gendered Cyber Harassment: A Growing Threat in the Digital Age*, 12 Indian J. Gender Stud. 56, 58–60 (2021).
[45] Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 347–49 (2014).
[46] Freedom House, *Freedom on the Net 2018: The Rise of Digital Authoritarianism* (2018), available at https://freedomhouse.org/report/freedom-net/2018.
[47] Information Technology Act, No. 21 of 2000, 66E, 67, INDIA CODE (2000); Indian Penal Code, No. 45 of 1860, 354D, 499, 509, INDIA CODE (1860)

faster takedown mechanisms, victim support systems, and digital literacy campaigns to educate users about their rights and online safety. It is also essential to challenge the cultural and societal mindset that blames or shames the victims, rather than holding perpetrators accountable.

Mobile Application-Based Crimes

With the widespread adoption of smartphones, tablets, and other portable digital devices, technology has become deeply embedded in everyday life. This increased dependence has inadvertently led to a rise in mobile application-based cybercrimes. Mobile platforms, especially Android, have become prime targets for cybercriminals due to their open-source nature and relatively lenient app submission policies. Cyber offenders exploit this by injecting malicious software into applications that appear legitimate, luring unsuspecting users into downloading malware-laden apps[48].

The Android operating system has frequently been the subject of malware infiltration, primarily due to the flexibility it offers developers in uploading apps. Malicious developers often take advantage of third-party app stores, which are less regulated compared to official platforms like the Google Play Store or Apple's App Store[49]. These alternative marketplaces become breeding grounds for cyber threats, distributing apps embedded with spyware, ransomware, or trojans designed to steal sensitive data, monitor user activity, or hijack device functions.

Even well-known app distribution platforms such as Apple's App Store, Windows Marketplace, and Blackberry World, while comparatively secure, are not entirely immune to such threats. The lack of robust vetting mechanisms in some platforms allows malicious apps to slip through the cracks. Additionally, companies that develop and manage applications often fail to implement adequate security safeguards[50], leaving apps vulnerable to exploitation. Once compromised, these apps can redirect users to phishing websites or collect personal and financial data without consent.

[48] *Symantec Corp.*, *Internet Security Threat Report* 17 (2019), https://symantec-enterprise-blogs.security.com (last visited July 17, 2025).
[49] *Kaspersky Lab*, *Mobile Malware Evolution 2020*, https://securelist.com/mobile-malware-evolution (last visited July 17, 2025).
[50] Brian X. Chen, *Malicious Apps Sneak Into Apple's App Store*, N.Y. Times (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/apple-app-store-security.html.

Cybercriminals also employ social engineering tactics such as sending fake emails, SMS messages, or push notifications that appear to come from trusted sources like banks or government agencies. These deceptive messages often contain links prompting users to download seemingly necessary applications or perform security updates[51]. In reality, these actions can lead to data breaches, identity theft, or unauthorized financial transactions.

Moreover, fraudulent applications often disguise themselves as legitimate utilities such as antivirus software, banking apps, or productivity tools deceiving users into granting permissions that compromise device security. Once installed, these malicious apps can gain access to **contacts, messages, banking credentials**, and even biometric data[52]. This not only threatens individual privacy but also endangers broader network systems, especially in professional or governmental environments.

To combat this growing threat, there is an urgent need for enhanced regulatory oversight, security audits, and consumer awareness campaigns. Developers should be required to follow strict guidelines for app development, and app marketplaces must employ advanced screening technologies to identify and remove harmful applications swiftly. Users, too, must remain vigilant avoiding downloads from unknown sources and verifying app legitimacy before granting access to sensitive data.

Right to Be Forgotten

The Right to Be Forgotten (RTBF) has emerged as a significant aspect of an individual's right to privacy, allowing a person to request the removal or restriction of access to their personal data, especially from public domains like the internet. It enables individuals to de-link, delete, limit, or correct the availability of their private information held by data fiduciaries, such as online platforms, organizations, or data controllers[53].

This concept first gained international attention through a 2014 landmark decision by the Court of Justice of the European Union (CJEU). The case involved Mario Costeja González, a Spanish citizen who contested that a simple search of his name on Google continued to display

[51] Interpol, *Cybercrime: Threats and Trends 2022*, https://www.interpol.int/en/Crimes/Cybercrime (last visited July 17, 2025).
[52] National Cyber Security Centre (UK), *Mobile Device Security Guidance*, Version 2.1 (2023), https://www.ncsc.gov.uk/collection/mobile-device-guidance (last visited July 17, 2025).
[53] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 143–47 (N.Y.U. Press 2004).

links to an old auction notice concerning his repossessed home. González argued that the information was no longer relevant and its continued visibility amounted to an invasion of his privacy. The CJEU ruled in his favor, recognizing that individuals could request the removal of outdated or irrelevant personal data from search engine results thus giving birth to what we now refer to as the "right to be forgotten[54]."

Following this, the European Union's General Data Protection Regulation (GDPR) formally incorporated the Right to Be Forgotten in Article 17, reinforcing that individuals have the right to request the erasure of personal data under specific circumstances, such as when the data is no longer necessary or was unlawfully processed[55].

In the Indian context, the Right to Be Forgotten has not yet been explicitly codified in legislation but has seen recognition through judicial pronouncements. In the case of Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. & Ors., the Delhi High Court addressed the issue in 2018. The petitioner sought the removal of certain allegedly defamatory content that affected his personal and professional life. The court acknowledged the Right to Be Forgotten as an integral part of the right to privacy, itself upheld as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy v. Union of India**[56]**. The Delhi High Court ordered a temporary restraint on the republication of the disputed material during the pendency of the suit, thereby validating the importance of the RTBF in protecting personal dignity and individual liberty.

Further attention to this right was drawn by Ashutosh Kaushik, a reality TV personality and winner of shows like Bigg Boss, who approached the courts seeking the removal of online content related to past incidents. Kaushik argued that such content continued to negatively affect his public image and personal life, and invoked the RTBF as a remedy. This highlighted the increasing relevance of the right in a digitally connected society where one's online history can have far-reaching and long-term consequences[57].

[54] Case C-131/12, *Google Spain SL v. Agencia Española de Protecctión de Datos (AEPD)* and *Mario Costeja González*, 2014 E.C.R. I-317.
[55] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1.
[56] *Zulfiqar Ahman Khan v. Quintillion Business Media Pvt. Ltd. & Ors.*, 2019 SCC OnLine Del 8494.
[57] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

In sum, while the Right to Be Forgotten is still evolving within the Indian legal framework, it underscores the growing need to balance the right to information with the right to privacy[58]. As digital footprints become increasingly permanent, empowering individuals to control their data visibility is becoming not just a legal issue but a deeply personal one as well.

Indian Legislations on Cybercrime: The Information Technology Act, 2000 and Its 2008 Amendment

India took a significant legislative step to address the evolving threats in the digital world with the enactment of the Information Technology Act, 2000 (IT Act, 2000). The primary aim of this law was to offer legal recognition to electronic transactions and facilitate the growth of e-commerce, e-governance, and e-banking. Beyond these goals, the Act also addressed cybercrimes, laying down penalties and legal procedures to deal with offenses committed using technology[59].

As technology advanced, so did the nature and complexity of cyber threats. To respond to these changes, the Information Technology (Amendment) Act, 2008 was introduced. This amendment expanded the scope of the original Act, introducing clearer definitions of cyber offenses and stronger mechanisms to enforce cyber laws. The combined framework of the 2000 Act and its 2008 amendment now forms the backbone of India's cyber legal regime[60].

Under this legislation, both civil and criminal liabilities are imposed for unauthorized access or damage to computer systems. For example:

- **Section 43** penalizes unauthorized access, downloading, introducing viruses, or damaging computer systems, with compensation liabilities.

- **Section 66** makes such acts punishable with imprisonment and fines when committed dishonestly or fraudulently.

[58] Rohan Abraham, *Ashutosh Kaushik Wants Past Fights Erased: Court Considers Right to Be Forgotten*, India Today (Apr. 15, 2021), https://www.indiatoday.in/law/story/ashutosh-kaushik-right-to-be-forgotten-delhi-hc1790575-2021-04-15.
[59] Information Technology Act, No. 21 of 2000, §§ 43, 66–66E, India Code (2000); Information Technology (Amendment) Act, No. 10 of 2009, India Code (2008).
[60] *S K.N. Govindacharya v. Union of India*, W.P. (C) No. 3672/2012 (Delhi High Court). *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

- **Section 66C** criminalizes identity theft, while Section 66D addresses cheating by personation using computer resources.

- **Section 66E** punishes electronic voyeurism, i.e., capturing or transmitting images of a person's private area without consent.

- While **Section 66A**, which dealt with offensive or harmful messages through communication service, was struck down by the Supreme Court in *Shreya Singhal v. Union of India* (2015), it remains a landmark in discussions on freedom of expression online[61].

A notable case in this domain is K.N. Govindacharya v. Union of India, decided in 2012. In this case, the petitioner raised concerns over the unrestricted access of minors (below the age of 13) to social networking platforms like Facebook and Orkut. The Delhi High Court observed that such platforms fall under the definition of "intermediaries" as per Rule 2(i) of the Information Technology (Intermediaries Guidelines) Rules, 2011. Accordingly, the court directed these companies to set clear privacy policies, user agreements, and grievance redressal mechanisms. It also emphasized the need for proper monitoring of user age and handling of complaints[62] within a reasonable time preferably within one month.

These provisions mark India's efforts to regulate the digital space, though challenges in enforcement and technological gaps still persist. Nonetheless, these laws lay the groundwork for addressing cybercrimes and protecting users in an increasingly digital world.

Data Privacy and Protection Law in India: The Digital Personal Data Protection Act, 2023

In a landmark development, India enacted its first comprehensive data protection law The Digital Personal Data Protection Act, 2023 (DPDP Act) in August 2023. This legislation represents a crucial step in establishing a legal framework for the collection, storage, and use of personal data in the digital age.

The journey toward this law was long and iterative. The process began in 2018, when an expert committee chaired by Justice B.N. Srikrishna submitted a draft Personal Data Protection Bill.

[61] Ministry of Electronics & Information Technology, National Cyber Security Policy, July 2, 2013, available at https://meity.gov.in.
[62] Pavan Duggal, *Cybersecurity in India: Evaluating the Promise and Pitfalls of National Policy* 14 (2024).

This was followed by the introduction of the Personal Data Protection Bill, 2019, which underwent extensive scrutiny by a Joint Parliamentary Committee. However, amid concerns about its complexity and implementation challenges, the bill was withdrawn in 2021. A revised version The Digital Personal Data Protection Bill, 2022 was introduced in November 2022[63], ultimately forming the basis of the DPDP Act, 2023.

The Act reflects a more streamlined approach to data regulation than its predecessor. It mandates that personal data can only be collected and processed with the individual's consent, except in specific situations such as for national interest, public order, or employment purposes. It also grants individuals key rights over their data, including:

- The right to access their personal information,
- The right to correct or update inaccuracies,
- The right to erase personal data under certain conditions, and Special protections for children's data.

Under the DPDP Act, data fiduciaries (entities that determine the purpose and means of processing personal data) are obligated to inform individuals about the purpose of data collection, limit usage to that purpose, and maintain reasonable security safeguards. Non-compliance with these obligations can result in financial penalties imposed by the Data Protection Board of India, the regulatory body created under the Act[64].

However, the Act has drawn both praise and criticism. Supporters see it as a long-awaited framework that balances user rights with innovation and ease of business. Critics, on the other hand, have expressed concern over the broad discretionary powers granted to the Central Government, particularly the power to exempt certain entities from compliance, and the lack of strong safeguards against government surveillance.

Nevertheless, the DPDP Act, 2023 sets a foundation for India's evolving data governance regime and aligns the country more closely with global data protection standards such as the

[63] Pranav Kumar, *Discretion and Data Security: The Critique of DPDP Act, 2023*, 28 Nat'l L.J. India 56, 58–60 (2024).
[64] Digital Personal Data Protection Act, 2023 §§ 12–13, 45; Data Protection Board of India, *Establishment & Functions*, https://dpb.gov.in.

EU's General Data Protection Regulation (GDPR)[65].

Conclusion

As India rapidly moves toward a digitally connected future, the challenges of cybercrime and data privacy are becoming more serious than ever. Our everyday lives be it banking, shopping, learning, or even social interactions are increasingly taking place online. With this shift, the risks have also grown: cyberattacks, identity theft, data breaches, and misuse of personal information are no longer rare incidents but everyday threats.

While the Information Technology Act, 2000, was a good starting point, it hasn't kept up with the times. New and evolving cyber threats like phishing, sextortion, cyberstalking, and child exploitation online are not adequately addressed under current laws. Many cyber offenses remain bailable, punishments are often too mild to be effective, and there's a lack of proper support for victims. Worse, there's no strong system in place for reporting bugs or loopholes in online platforms, leaving users and organizations vulnerable.

What India needs now is not just stronger laws, but smarter ones. Laws must be updated to reflect the reality of today's online risks and ensure stricter penalties for offenders. More importantly, privacy must be treated as a basic right, not just an afterthought. People deserve control over how their personal data is collected, used, and shared. The Digital Personal Data Protection Act, 2023, is a step in the right direction, but implementation will be key.

India should also look outward working with other countries and joining international treaties like the Budapest Convention on Cybercrime can improve our ability to track and stop cross-border cyber criminals.

At the heart of all this must be one core principle: people come first. Protecting digital rights, securing data, and ensuring accountability must become part of our digital growth story. Only then can India create a safe, trustworthy, and inclusive digital space for all.

[65] Pranav Kumar, *Discretion and Data Security: The Critique of DPDP Act, 2023*, 28 Nat'l L.J. India 56, 58–60 (2024).

REFERENCES

1. The Information Technology Act, No. 21 of 2000, § 66, Acts of Parliament, 2000 (India).

2. The Information Technology (Amendment) Act, No. 10 of 2009, Acts of Parliament, 2009 (India).

3. Ministry of Electronics & Information Technology, *National Cyber Security Policy* (July 2, 2013), https://meity.gov.in.

4. Gaurav Saluja, *Critical Assessment of the Information Technology Act, 2000 and Its Amendment, 2008* (Apr. 2023) (unpublished manuscript), https://ssrn.com/abstract=5262168.

5. Priya Rao, Cyber Crime and Related Laws in India, 7(1) *Int'l J. Rev. & Res. Soc. Sci.* (2019),https://ijrrssonline.in/HTMLPaper.aspx?Journal=International+Journal+of+Reviews+and+Resea rch+in+Social+Sciences;PID=2019-7-1-48.

6. Sudhanshu Sekhar Tripathy, *A Comprehensive Survey of Cybercrimes in India Over the LastDecade*, arXiv (May 2025), https://arxiv.org/abs/2505.23770.

7. Ministry of Electronics & Information Technology, *National Cyber Security Policy*, Government of India (July 2, 2013).

8. Sameeksha Shetty, *Digital Predators: The Legal Landscape of Child Pornography in India*, SSRN (Oct. 20, 2024), https://ssrn.com/abstract=5051692.

9. Niranjana K. & Murugan Ramu, A Study on Cyber Child Pornography in India, *Psychology & Education J.*, Apr. 2021, https://www.researchgate.net/publication/351022212.

10. Satyam Mangal, *Safeguarding Digital Childhood: A Critical Analysis of the IT Act, 2000 in Addressing Cyberbegging and Sharenting*, *Indian J. L. & Tech.* (May 2025), https://nluo.ac.in/storage/2025/05/9.-Safeguarding-Digital-Childhood.

11. The Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).

12. Ministry of Electronics & Information Technology, *Intermediary Guidelines and Digital Media Ethics Code Rules, 2021*, G.S.R. 139(E) (Feb. 25, 2021), https://www.meity.gov.in.

13. National Cyber Security Policy-2013, Department of Electronic and Information Technology, available at https://nciipc.gov.in/documents/National_Cyb er_Security_Policy-2013.pdf,

14. United Nations Human Rights Office of the High Commissioner, "Convention on the Rights of the Child", available at https://www.ohchr.org/en/professionalinterest/ pages/crc.aspx Adrian Shahbaz, "The Rise of Digital Authorization", Freedom House, October 2018.