# Victimology in Digital Age

**Dr. Kalpana Thakur**

**Assistant Professor, University School of Law, Rayat Bahra Professional University, Hoshiarpur**

**DOI: https://dx.doi.org/10.47772/IJRISS.2025.908000360**

**Received: 10 August 2025; Accepted: 16 August 2025; Published: 11 September 2025**

## ABSTRACT

The exponential growth of the internet, mobile technologies, and social media platforms has transformed communication, commerce, and social interaction but has also created unprecedented opportunities for digital victimization. Victimology in the Digital Age explores the evolving nature of victimization in cyberspace, where anonymity, transnational reach, and rapid content dissemination heighten the vulnerability of individuals and communities. This study examines the forms of digital victimization-including cyberstalking, online harassment, non-consensual dissemination of intimate images, financial phishing scams, child sexual exploitation, and identity theft-while highlighting the psychosocial, economic, and reputational harms inflicted upon victims. The paper analyzes domestic legal frameworks such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023 (formerly IPC), the Protection of Children from Sexual Offences (POCSO) Act, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as well as landmark judicial decisions like Shreya Singhal v. Union of India and Justice K.S. Puttaswamy (Retd.) v. Union of India. Further, it evaluates international norms and standards, including the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985), to identify best practices for victim protection. Special emphasis is placed on the rights of digital victims, including access to justice, protection from secondary victimization, privacy, compensation, rehabilitation, and participation in legal processes. The study argues for multi-layered state obligations beyond prosecution, encompassing legislative reform, victim support services, capacity-building of law enforcement, and public-private partnerships with technology platforms for rapid takedown of harmful content. Through a victim-centric approach, the paper underscores the need for a robust accountability ecosystem that balances constitutional freedoms with the imperative to protect victims in cyberspace. By integrating jurisprudential developments, comparative perspectives, and practical strategies, this research aims to provide a comprehensive framework for addressing digital victimization and safeguarding the dignity and rights of victims in the information age.

**Keywords:** Victimology, digital victimization, cybercrime, privacy, victim rights, India, Information Technology Act, online harassment

## INTRODUCTION

The advent of the digital age has revolutionized virtually every aspect of human life, from communication and commerce to education, governance, and interpersonal relationships. Technology has brought the world closer, collapsed distances, and redefined the notions of access and convenience. Social media platforms, instant messaging services, digital banking, e-commerce websites, and video conferencing tools have become integral to everyday existence. However, this unprecedented technological expansion has also opened new frontiers for criminal behavior, leading to the emergence of a parallel domain of victimization. This domain, characterized by anonymity, border lessness, and rapid scalability, presents novel challenges to law enforcement, policy makers, and scholars alike.

Traditionally, victimology has focused on understanding the nature and rights of victims of heinous crimes. These crimes were often constituted in physically with visible harm and identifiable damages. Victim responses and justice mechanisms are based on the physical, materiality and observable nature of these acts. With the rise of the

digital world, the drawn boundary of crime and victimization has vastly grown. Individuals are now vulnerable to such crimes or acts that occur entirely within virtual environments. The transition from the physical to the digital has required to be redesigned.

The digital age comes with a digital type of threats: cyberstalking, identity theft, revenge pornography, data breaches, phishing scams, and online defamation. Unlike traditional crimes, these acts often leave no physical trace and are perpetrated by individuals who can easily conceal their identities using technology. Moreover, the global natures of the internet create new issue of jurisdictional authority, as crimes may be committed in one country and affect victims in another. As a result, victims often find themselves helpless of legal support. This necessitates a re-evaluation of how victimhood is understood and addressed in current criminology.

In this context, digital victimology emerges as a specialized sub-discipline that focuses on the new type of harm in the cyberspace. It examines how digital infrastructure supports crime, the patterns of victimization unique to virtual environments and the effectiveness of existing legal and institutional responses. Digital victimology also explores the psychosocial dimensions of victimhood, how victims process trauma, deals with stigma and seek justice in an ecosystem that often promotes speed over safety and profit over protection.

This paper aims to provide a comprehensive overview of victimology in the digital age, focusing on evolving patterns of digital harm, legal frameworks such as the Information Technology Act, 2000 and relevant provisions of the Indian Penal Code, and the institutional mechanisms available for redressal. It also criticizes the effectiveness of these systems and explores avenues for reform. By adopting a multidisciplinary approach that includes legal analysis, sociological insights, and victim-centered perspectives, this study contributes to a deeper understanding of how the digital revolution is reshaping the landscape of victimization and what must be done to safeguard dignity, privacy, and justice in a technologically driven society.

**Types of Digital Victimization**

The landscape of digital victimization is vast and continually evolving. Below are the major types of offenses that define victimology in the cyber age:

**Cyberstalking:**

Cyberstalking is the persistent harassment or threatening behavior by an individual using digital communication tools. Victims of cyberstalking often experience emotional distress and fear for personal safety.

Example: A woman in Mumbai was stalked by her ex-boyfriend through emails and fake social media profiles. He sent explicit content to her friends and family and tracked her movements using GPS technology.

Case Law: In the case of Manik Taneja v. State of Karnataka (2015), the Supreme Court held that online expressions critical of public authorities must be assessed carefully, especially in light of the accused's intent and the threat to public order.

**Online Harassment and Trolling:**

Repeated, targeted abuse or threats directed at individuals, often on social media platforms. Harassment may be gendered, racist, caste-based, or political. It can include doxxing (publishing private information), hate speech, and threatening messages.

This includes unwelcome sexual advances, demands for sexual favors, or online content that demeans the dignity of women and marginalized genders. It may occur via email, chat platforms, forums, or social media.

Example: The 'Boys Locker Room' incident in India involved schoolboys sharing obscene pictures of girls and discussing sexual violence.

Legal Framework: Section 354A of IPC and Section 67 of the IT Act deal with sexually explicit content and harassment.

Case Law: Shreya Singhal v. Union of India (2015) played a vital role in clarifying freedom of expression and misuse of Section 66A of the IT Act.

**Cyberbullying:**

Particularly prevalent among adolescents, cyberbullying involves online behavior intended to intimidate, shame, or demean individuals, often through social media or messaging platforms. Studies show it contributes to depression, anxiety, and suicide ideation among youth.

Example: In Hyderabad, a 13-year-old died by suicide after being bullied for his appearance in an online gaming forum.

Legal Reference: While India does not have a specific anti-bullying law, provisions under the IPC and Juvenile Justice Act can be invoked.

**Revenge Pornography (Non-Consensual Intimate Imagery):**

Revenge porn involves sharing or threatening to share intimate images or videos without consent. It is a form of sexual exploitation and causes severe emotional damage.

Example: In Kerala, a woman committed suicide after her ex-partner uploaded their private video online.

Legal Provision: Section 66E of the IT Act, 2000 criminalizes the violation of privacy by capturing, publishing, or transmitting private images without consent.

**Identity Theft and Impersonation:**

The fraudulent use of another person's personal data, including financial information, social security numbers, or images, often for criminal gain or reputational damage

Cybercriminals can steal personal details such as Aadhaar numbers, bank details, or social media logins to impersonate individuals and commit fraud.

Example: In Delhi, a man was defrauded of ₹1.2 lakh after sharing his OTP with a person posing as a bank executive.

Legal Protection: Sections 66C and 66D of the IT Act deal with identity theft and cheating by impersonation using computer resources.

**Online Financial Frauds and Phishing:**

Victims are tricked into revealing sensitive information like bank credentials or OTPs. Financial scams have increased manifold with the proliferation of UPI, e-wallets, and online banking.

**1) Phishing / Smishing / Vishing**

Fraudsters pose as a bank, RBI/Income-Tax/NPCI, courier, or e-commerce support to make you click a link, open an attachment, or share OTPs/card details on call. Variants include fake KYC re-verification, "account blocked," undelivered package, electricity bill disconnection, or tax refund. These aim to harvest credentials or push you into authorizing a transaction. CERT-In has repeatedly flagged such campaigns.

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume IX Issue VIII August 2025

**UPI scams**

- "Collect request" trap: You're told you'll receive money but are pushed to "approve" a collect request in your UPI app-approving actually pays the fraudster.
- QR-code 'quishing': You scan a QR sent by a stranger to "get paid." Scanning can open a phishing page, auto-launch a collect request, or plant malware. CERT-In has warned specifically about QR code phishing. NPCI advises never to scan unknown QR codes or disclose UPI PIN/OTP.

**Remote-access/screen-sharing apps**

Callers (posing as "customer care") get you to install a remote tool; they watch your screen, read OTPs, change UPI PINs, or trigger payments. NPCI explicitly warns against using such apps during financial transactions.

**OTP relay & card-not-present frauds**

Fraudsters social-engineer OTPs or 3-D Secure prompts to complete card/UPI transactions in real time. RBI's two-factor norms help, but social engineering defeats them if you share OTP/PIN.

**SIM-swap / number takeover**

Your mobile number is illicitly ported/duplicated; incoming OTPs now reach the fraudster. Often preceded by targeted phishing/vishing.

**Investment/job task"/loan-app rackets**

High-return crypto/stock groups, part-time "rate & review" tasks, or predatory loan apps that coerce repayments using contact scraping and threats. These mix phishing + extortion techniques and frequently route funds through mule accounts.

**2) Red flags you can spot quickly**

- Urgent threats ("account frozen," "power cut in 30 minutes"), secrecy demands, or too-good-to-be-true returns.
- Links with odd spellings, shortened URLs, or domains not matching the real institution.
- Anyone asking for OTP/UPI PIN/APP passcode, or to approve a collect request to "receive" money.
- Requests to install screen-sharing/remote-access apps, or to read out your SMS alerts. NPCI's guidance: **never** share credentials or transact while on a call with a third party.

**3) If money has just moved: the first-hour drill**

1. Call 1930 immediately (Cybercrime Helpline). Ask for CFCFRMS (Citizen Financial Cyber Fraud Reporting & Management System) ticketing* so the beneficiary bank can try to freeze funds. Then file the online complaint on the National Cybercrime Reporting Portal (NCRP). These are official Government of India channels.
2. Inform your bank right away (via official app/number printed on card/website). Ask for dispute/chargeback where applicable and account monitoring/hold.
3. Preserve evidence: screenshots, SMS alerts, call logs, UPI transaction IDs, phishing URLs, QR images, and the handle you interacted with.
4. File an FIR/e-FIR at the nearest police station/cyber-PS; cite Information Technology Act Sec 66C (identity theft) and Sec 66D (cheating by personation using computer resource), plus cheating under the Bharatiya Nyaya Sanhita (successor to IPC 420). (BNS maps cheating from old IPC Sec 420 to BNS Sec 318.)

Why speed matters: The banking system tries to ring-fence suspect credits quickly. Many states report substantial amounts frozen because victims called 1930 promptly.

**4) Your financial remedy with banks (RBI rules)**

- RBI's "Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions" (circular DBR.No. Leg.BC.78/09.07.005/2017-18, July 6, 2017) sets when the bank bears the loss vs. the customer—depending on whether the fault was bank/systemic, third-party breach, or customer negligence, and how quickly you report. Early reporting (often within 3 days) maximizes your protection. Check your bank's board-approved policy aligned to this RBI circular
- If the bank does not resolve your complaint in 30 days or you're dissatisfied, escalate to the RBI Integrated Ombudsman Scheme (RB-IOS, 2021)-a cost-free, "One Nation, One Ombudsman" mechanism.

**5) Legal framework you can rely on**

- IT Act, 2000
  - Sec 66C- identity theft (e.g., misuse of your password/credentials).
  - Sec 66D - cheating by personation using a computer resource (typical for vishing/phishing).
- Bharatiya Nyaya Sanhita (BNS), 2023
  - Cheating/dishonest inducement (mapped from IPC 420 → BNS Sec 318), plus other property/forgery offences as facts warrant. Use BNS for offences on/after July 1, 2024; legacy IPC applies to older acts.

**6) Prevention: practical checklists**

For individuals

- Never share OTP/UPI PIN/app passcodes, and never approve a collect request to "receive" money. (Receiving needs no PIN.)
- Use official apps and bookmarks; avoid links in SMS/WhatsApp/email.
- Do not install or keep remote-access/screen-sharing apps on phones used for banking.
- Verify phone numbers and do not call back numbers in SMS; use the number on your bank card/website.
- Prefer WebAuthn/FIDO2 or app-based authenticators for email/brokerage; keep devices updated; enable transaction alerts.
- For UPI, set lower daily limits, and consider using a separate low-balance account for everyday payments.

For small businesses & institutions

- Enforce least-privilege access to banking portals; restrict who can approve payments.
- Train staff to spot phishing and QR-code traps; run simulated phishing drills.
- Use email authentication (SPF/DKIM/DMARC) and attachment/link sandboxing.
- Keep a runbook with bank hotlines, 1930, and NCRP links for immediate escalation.

Special notes on QR & UPI

- Scanning a QR is usually to pay, not to receive. Treat any "scan to receive" instruction as suspect. CERT-In has flagged QR-code phishing (quishing) patterns.
- Never transact while on a call with anyone "guiding" you. NPCI advises to avoid posting grievance details publicly and to stop transactions if anything feels rushed.

**7) How to write your police/bank complaint (quick template)**

- Facts in order: date/time, channel (UPI/card/net-banking), amount, beneficiary details (UPI ID/account/IFSC), reference/UTR, how contact occurred (SMS/call/link/QR), what was shared/approved, and what you did after (1930 call, tickets, bank intimation).
- Offences cited: IT Act Sec 66C/ Sec 66D; BNS cheating (mapped from IPC 420 → BNS §318); add forgery/falsification if applicable. Attach screenshots, call logs, SMS headers, email headers.

**8) Where to report & track**

- Immediate hotline:1930 (request CFCFRMS escalation).
- Online: National Cybercrime Reporting Portal-file a complaint and upload evidence; you can track status after obtaining the reference number
- Banking grievance: Write to your bank's nodal officer referencing the RBI 2017 liability circular; escalate to the RBI Ombudsman (RB-IOS, 2021) if unresolved in 30 days.

**Child Sexual Exploitation and Grooming:**

Offenders use digital platforms to lure, groom, and exploit minors. The Protection of Children from Sexual Offences (POCSO) Act and IT Act have provisions against the digital exploitation of children.

**Cyber Trafficking and Online Recruitment for Exploitation:**

Victims are trafficked or recruited online for labor or sexual exploitation, often under false pretenses or through coercion.

**Digital Hate Crimes:**

Crimes motivated by hate based on religion, caste, gender, or sexuality, which are perpetrated via online platforms. These include fake news, communal incitement, and targeted digital propaganda.

Each form of digital victimization reflects the misuse of technology and the failure of existing frameworks to adequately anticipate or address evolving criminal patterns. A multidisciplinary and rights-based approach is necessary to identify victims, protect their interests, and ensure access to justice.

**Doxxing:**

Doxxing is the act of publishing private, identifying information about an individual without their consent, usually with malicious intent.

Example: Female journalists and activists have been victims of coordinated online doxxing campaigns, leading to threats and abuse.

Legal Reference: Doxxing violates privacy rights and may attract charges under IPC Sections 500 (defamation), 504, 506, and the IT Act.

**Legal and Jurisprudential Frameworks:** The evolution of digital victimology has prompted a corresponding development in legal instruments, both internationally and domestically. Legal frameworks provide not only punitive mechanisms but also preventive and remedial measures to protect the rights of victims in cyberspace.

- International Legal Frameworks: Several international treaties and conventions implicitly or explicitly address digital crimes and victim rights:
- The Council of Europe's Budapest Convention on Cybercrime (2001) is the first international treaty seeking to address internet and computer crime by harmonizing national laws and enhancing investigative techniques. Although India is not a signatory, it remains influential in shaping global norms.
- The Universal Declaration of Human Rights (UDHR) and International Covenant on Civil and Political Rights (ICCPR) affirm the right to privacy, protection from degrading treatment, and freedom of expression. These principles are increasingly interpreted to apply to digital environments.
- The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) obliges states to take appropriate measures to eliminate violence against women, including online abuse and harassment.
- The Convention on the Rights of the Child (CRC) provides the framework for protecting children from online sexual exploitation, grooming, and cyberbullying.

**Domestic Legal Frameworks in India**:

**Information Technology Act, 2000 (IT Act)**

The IT Act is India's core "cyber law." Beyond recognizing electronic records, it creates specific computer and content offences and a regulatory spine (blocking powers, safe-harbour for intermediaries, CERT-In, etc.). Key sections you listed:

- Sec 66C - Identity theft

Punishes fraudulent use of another person's electronic signature, password, or any unique ID. Penalty: up to 3 years' imprisonment and fine up to ₹1 lakh.

Example: Logging into someone's email/social account with their password and performing actions as them.

- Sec 66D - Cheating by personation using a computer resource

Covers impersonation scams (e.g., bogus bank/UPI support, "work-from-home" job frauds). Penalty: up to 3 years and fine up to ₹1 lakh.

- Sec 66E - Violation of privacy

Criminalizes capturing, publishing, or transmitting images of a person's private areas without consent in circumstances violating privacy.

Penalty: up to 3 years and/or fine up to ₹2 lakh.

Example: Circulating a secretly recorded changing-room clip.

- Sec 67A - Publishing/transmitting sexually explicit content in electronic form

Targets sexually explicit material (consensual adult content still falls here if unlawfully published/transmitted). Penalty: first conviction up to 5 years + fine up to ₹10 lakh; subsequent up to 7 years + fine up to ₹10 lakh.

Important related section:67B specifically targets child sexual abuse material (CSAM) - including creating, browsing, downloading, advertising or distributing such material.

Note: Sec 66A (sending "offensive" messages) was struck down by the Supreme Court in Shreya Singhal v. Union of India (2015). It no longer exists; do not invoke it. The Court also read down Sec 79 and upheld Sec 69A (blocking).

Platform-facing spine in the IT Act:

- Sec 69A - Central Government's power to block public access to information (with prescribed safeguards). Non-compliance can attract up to 7 years.

- Sec 79 - Safe-harbour for intermediaries for third-party content, conditional on due diligence and timely action under the Rules (and on court/government orders after Shreya Singhal).

- Sec 70B - Establishes CERT-In as national incident-response agency. (Useful when cyber incidents overlap with criminal investigations.)

2) Indian Penal Code, 1860 → now Bharatiya Nyaya Sanhita (BNS), 2023

**From 1 July 2024, the IPC has been replaced by the BNS for new offences. The provisions you cited map as follows:**

| IPC (old) | Subject | BNS (New) | What it covers (New) |
|---|---|---|---|
| Sec 354D | Stalking | Sec 78 | Includes monitoring a woman's use of the internet, email, or other electronic communication; 1st conviction up to 3 years, repeat up to 5 years + fine. |
| Sec 509 | Word, gesture, act intended to insult modesty of a woman | Sec 79 | Includes intrusion upon privacy and acts done online (e.g., lewd DMs, doxxing intended to insult); simple imprisonment up to 3 years + fine. |
| Sec 499-500 | Defamation | Sec 356 | Consolidates defamation; adds **community service** to punishment options. (Use BNS Sec 356 now; IPC Sections 499-500 apply to acts before 1 July 2024.) |

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

POCSO is **technology-neutral** but expressly covers conduct committed **"through any medium… internet or any other electronic form."** The provisions most used in **digital sexual abuse of children**:

- **Sec11–12 (Sexual harassment):** Includes **showing any object in any form or media for pornographic purposes**, repeatedly **following/watching/contacting a child through electronic or digital means**, or **threatening to use real/fabricated depictions**. **Punishment:** up to **3 years + fine**.
- **Sec13–15 (Use of child for pornographic purposes; storage/possession):** Criminalizes **production, offering, transmitting, publishing, facilitating, distributing**, and even **possession** of CSAM (with graded penalties, including minimums introduced in 2019).
- **Sec 9–21 (Reporting): Mandatory reporting** to SJPU/local police; liability for **failure to report**. Very important for platforms/schools/Studios and anyone encountering CSAM.

**Overlap with IT Act:** POCSO Sections 13-15 and IT Act **Sec 67B** often run **together** - Sec 67B captures the electronic dimension (creation, browsing/downloading, advertising/distribution), while POCSO focuses on the **child-protection core** with higher minimums and child-friendly procedures (Special Courts, in-camera trials).

IT (Intermediary Guidelines & Digital Media Ethics Code) Rules, 2021 (as amended in 2022 & 2023)

These Rules supply the due-diligence that intermediaries must follow to retain §79 safe-harbour. High-level duties include:

Core due-diligence timelines (Rule 3)

- 72 hours: On lawful request, an intermediary must furnish information/assistance to law-enforcement as soon as possible, but not later than 72 hours.
- 24 hours (NCI/impersonation): Remove/disable content that prima facie exposes private areas, shows full/partial nudity, depicts a sexual act, or is impersonation (including AI-morphed images) within 24 hours of a complaint by the affected person or someone on their behalf.
- Grievance handling: Acknowledge within 24 hours and resolve within 15 days; many categories (other than NCI) carry an expedited 72-hour resolution requirement after 2022 amendments.
- Unlawful content on order: Where there is a court/Government order, platforms must remove/disable within 36 hours (as explained in practitioner summaries).

**B. Significant Social Media Intermediary (SSMI) obligations (Rule 4)**

Platforms with **> 50 lakh (5 million) registered users in India** must, inter alia:

- Appoint an **India-based Chief Compliance Officer**, **Nodal Contact (24×7)**, and **Resident Grievance Officer**.
- **Publish monthly compliance reports**, **enable traceability** of the **first originator** for specified serious offences (via judicial/§69 orders), and **deploy tech measures** to proactively detect **rape/CSAM "exact matches"** with human oversight.

**Interaction with** Shreya Singhal**:** Content takedown "upon actual knowledge" has been aligned with **court orders or government notices**; blanket "user complaint = legal knowledge" is not sufficient for loss of safe-harbour (except the **24-hour NCI/impersonation** lane created by the Rules).

**How these frameworks work together (typical charging & compliance patterns)**

1. Revenge-porn / non-consensual intimate imagery (NCI):
    - IT Act Sec 66E (privacy) + Sec 67/67A (obscenity/sexually explicit) and, if a child is involved, Sec 67B + POCSO Sections 13–15.
    - Platforms must remove within 24 hours once the survivor (or representative) flags it; LEA can also seek identities/logs within 72 hours. Blocking may be invoked under Sec 69A for systemic takedowns.
2. Cyberstalking/online harassment of women:
    - BNS Sec78 (stalking by online monitoring), BNS Sec 79 (insulting modesty incl. intrusion upon privacy), with IT Act Sec 66E when images are involved; add Sec 67 if obscene transmissions occur.
3. Financial impersonation scams ("customer care," KYC links, fake job offers):
    - IT Act Sec 66D (cheating by personation using computer resource), Sec 66C (identity theft), and theft/fraud sections of BNS as applicable. Intermediaries may need to preserve data (Sec67C) and assist under 72-hour timeline.
4. CSAM cases:
    - IT Act Sec 67B + POCSO Sections 13–15 and procedural safeguards under POCSO (Special Courts, reporting). Platforms should proactively hash-match exact CSAM, remove rapidly, and report/assist.

**Evidence: electronic records under the Bharatiya Sakshya Adhiniyam (BSA), 2023: Since July 2024, the BSA replaced the Indian Evidence Act. Two quick anchors you'll rely on:**

- **Sec 63 BSA**- lays down **admissibility of electronic records** (functional successor to old Sec 65B), including the **certificate requirement**; official IndiaCode page is now live.
- BSA also clarifies the status of electronic/digital records as documents/primary evidence in certain scenarios (see BSA text). This matters for social-media chats, device extractions, server logs, hash values used in cybercrime trials.

**Practical compliance / investigation checklist**

- **Jurisdiction & FIR:** Cyber offences can be registered where the **information/computer resource** is targeted or where the **victim resides** (Cr.P.C/Bharatiya Nagarik Suraksha Sanhita tools apply).
- **Preservation:** Seek **Sec 67C IT Act** preservation from platforms and **expedited disclosure** within **72 hours** under the Rules.
- **Takedown vs. blocking:** Use **Rule 3 / Rule 4** pathways for takedown; escalate to **Sec 69A** for **systemic blocking** (multiple mirrors/links).
- **Charging strategy:** Where the victim is a **child**, **always add POCSO** counts in addition to IT Act offences. For **women-targeted harassment**, add **BNS Sections 78/79** as warranted.

- **Evidence packaging:** Ensure **Sec 63 BSA certificate** accompanies prints/exports of chats, emails, logs, or captures; maintain chain of custody.

**Jurisprudential Developments**: Indian courts have played a pivotal role in shaping the legal framework and ensuring accountability for cyber victimization. Through progressive decisions, the judiciary has addressed the challenges posed by the digital environment, balancing individual rights with societal interests. Some landmark cases are discussed below:

**Shreya Singhal v. Union of India (2015)**

This case is considered a watershed moment in India's cyber law jurisprudence. The petition challenged the constitutionality of Section 66A of the Information Technology Act, 2000, which criminalized sending "offensive messages" through communication services. **Judgment:** The Supreme Court struck down Section 66 A as unconstitutional on the grounds that it was vague, overbroad, and capable of misuse offensive and annoyance which were not clearly defined, leading to arbitrary arrests and suppression of free speech.

**Significance:**

- It reaffirmed Article 19(1)(a) of the constitution of India as a fundamental right and underscored that any restriction must be reasonable and fall within the narrow ground mentioned in Article 19 (2). At the same time, the judgement recognised that cyber victimization and online harassment are genuine concerns. It suggested that the government could craft precise and narrowly-tailored laws to combat digital crimes without encroaching on constitutional freedoms.
- **Impact:** This decision strengthened safeguards against misuse of cyber laws by law enforcement agencies and emphasized the importance of protecting online expression while simultaneously urging the need to address abuse in the digital space.

**2. Kamlesh Vaswani v. Union of India (2013)**

In this case, the petitioner sought a complete ban on pornographic websites, arguing that easy access to such content was a major cause of sexual violence and cyber victimization, particularly against women and children.

**Judgment:**

The Supreme Court did not fully accept the plea for a total ban. However, it did recognize that unrestricted access to pornographic content can have a detrimental effect on society, especially minors.

**Significance:**

The Court's observations opened a broader debate on how far the State can regulate online content without infringing fundamental rights. It prompted the government to explore regulatory mechanisms, such as targeted blocking of child sexual abuse material (CSAM) and obscene content under Section 69 A of IT Act and the Intermediary Guidelines now IT Rules.

**Impact:**

The case highlighted the complexities in balancing morality, public order and privacy rights, and the need for a nuanced regulatory framework instead of a blanket ban. It also paved the way for proactive monitoring and blocking of unlawful content by intermediaries.

**In Re: Prajwala Letter Case (2015)**

This case originated from a letter written by NGO Prajwala to the Supreme Court, enclosing a pen drive containing rape videos that were circulating online. The Court treated the letter as suo motu proceedings to address the larger issue of sexual violence content being shared on the internet.

**Judgment & Directions:**

- The Supreme Court issued detailed directions to the Union Government, law enforcement agencies, and internet intermediaries to curb the circulation of rape and child sexual abuse videos online.
- It mandated that social media platforms and search engines develop proactive mechanisms-such as hash-matching technologies and keyword-based blocking—to detect and remove non-consensual sexual content.
- The Court further emphasized the necessity of protecting the identity and dignity of victims, underscoring the importance of Section 228A of the Indian Penal Code (now Section 71 of the Bharatiya Nyaya Sanhita, 2023), which prohibits the disclosure of a rape victim's identity.

**Significance:**

- This case marked a significant shift from reactive to preventive strategies in combating digital victimization.
- It set a precedent for collaborative efforts between the judiciary, the government, and internet intermediaries in establishing effective technical measures for the protection of victims.

**Broader Impact:**

- These cases collectively underscore that cyber victimization poses a serious threat to individual dignity and societal order.
- They reflect the judiciary's dual approach.
- Protect constitutional freedoms-particularly the right to free speech-by striking down vague or disproportionate laws (Shreya Singhal v. Union of India).
- Mandate preventive measures from the State and private intermediaries to curb digital crimes (In Re: Prajwala Letter Case).

The jurisprudence also recognizes the evolving nature of cyber threats and the need for constant legal adaptation to emerging technologies and online behaviours.

**Jurisprudential Developments on Digital Victimization in India**

The jurisprudential developments around digital victimization in India illustrate the judiciary's efforts to balance competing interests—freedom of expression, privacy, dignity, and public morality. These decisions have laid the foundation for robust accountability mechanisms, clearer legislative drafting, and collaborative strategies for the prevention and investigation of cybercrimes. As online spaces continue to expand, judicial oversight remains essential to ensure that victims of cybercrimes receive justice without compromising fundamental rights.

**Victim Rights and State Obligations in the Digital Age**

As digital victimization escalates, the State bears both a constitutional and international obligation to protect, rehabilitate, and empower victims. Victim rights are anchored in Articles 14, 19, and 21 of the Indian Constitution, international human rights norms, and victim-centric jurisprudence. These rights encompass access to justice, protection and privacy, compensation, rehabilitation, and participation in the legal process.

**Right to Access Justice**

Victims of cybercrimes often face institutional and infrastructural hurdles, such as a lack of cybercrime expertise in police stations, delays in FIR registration, and inadequate digital reporting mechanisms.

- **Constitutional Guarantee:** Article 21 of the Indian Constitution guarantees the right to life and personal liberty, judicially expanded to include the right to a fair, effective, and timely trial.
- **Mandatory FIR Registration:** In Lalita Kumari v. Government of Uttar Pradesh (2014) 2 SCC 1, the Supreme Court held that registration of an FIR is mandatory in cognizable offences, leaving no discretion

to the police. This principle applies directly to cyber offences such as cyberstalking, cyberbullying, and revenge pornography.

- **Practical Mechanisms:**
    - The National Cyber Crime Reporting Portal (https://cybercrime.gov.in) enables online filing of complaints.
    - Many states operate 24×7 cybercrime helplines and dedicated cyber cells with trained personnel for rapid assistance.

**Right to Protection and Privacy**

Digital victims-particularly those whose intimate images or personal data are disseminated online-face an acute risk of secondary victimization.

- **Privacy as a Fundamental Right:** In Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1, a nine-judge bench of the Supreme Court recognized the right to privacy as a fundamental right under Article 21. This obligates the State to safeguard victims' identities and personal data from unwarranted exposure.

- **Statutory Safeguards:**
    - Section 228A IPC (now Section 71 of the Bharatiya Nyaya Sanhita, 2023) prohibits disclosure of a rape victim's identity. Courts have extended this principle to cybercrimes involving sexual victimization.
    - The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate that intermediaries remove intimate content within 24 hours of receiving a victim's complaint.

**Right to Compensation and Rehabilitation**

Victims are entitled to financial and psychological support to aid recovery.

- **Criminal Procedure Code Provision:** Section 357A of the Code of Criminal Procedure, 1973 mandates each State to establish victim compensation schemes in coordination with State Legal Services Authorities (SLSAs).

- **Special Schemes:**
    - Delhi State Legal Services Authority (DSLSA) offers targeted compensation for victims of online sexual exploitation.
    - Maharashtra and Karnataka have incorporated cyber sexual abuse victims into their victim compensation frameworks.

- **Rehabilitation Measures:** Include psychological counselling, social reintegration, and economic assistance, especially for victims facing job loss or social stigma.

**Right to Participation in Legal Processes**

Victims should be treated as active participants in criminal proceedings rather than passive witnesses.

- **Malimath Committee Recommendations (2003):** Advocated for victims' rights to be heard at crucial stages of criminal proceedings (e.g., bail, sentencing) and recommended reforms to recognize victims as stakeholders.

- **Judicial Practices:** Victims (or their legal representatives) can:
    - Submit victim impact statements.
    - Receive regular updates on case progress.
    - Challenge decisions such as bail orders and acquittals.

**International Norms and Standards**

- **United Nations Framework:** The UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power (1985) obligates States to ensure access to justice, provide restitution, compensation, and support services, and adopt measures to prevent secondary victimization.
- **Global Cybercrime Standards:** International conventions, such as the Budapest Convention on Cybercrime (2001), though not ratified by India, emphasize victim-centric frameworks in cybercrime response.

**Broader State Obligations Beyond Punishment**

A rights-based approach requires the State to go beyond prosecuting offenders:

1. **Preventive Education:** Conduct nationwide awareness campaigns on digital safety, with a focus on vulnerable groups such as women and children.
2. **Capacity-Building:** Train police, prosecutors, and judges in cyber forensic techniques and victim-sensitive approaches.
3. **Public–Private Partnerships:** Collaborate with technology companies, NGOs, and international agencies for swift removal of harmful content.
4. **Transparency:** Publish data on cybercrime cases, compensation granted, and rehabilitation outcomes to build public trust.

## CONCLUSION

Victim dignity in the digital age is both a constitutional guarantee under Article 21 and an international obligation. Through landmark rulings such as Lalita Kumari, Puttaswamy, and the recommendations of the Malimath Committee, Indian jurisprudence has progressively strengthened victims' rights. However, true victim empowerment requires systemic reforms, stronger enforcement, and multi-agency coordination to address the evolving challenges of cyber victimization.

## REFERENCES

1. CERT-In. (2023, August). Advisory on QR code phishing (quishing) campaigns in India (CIAD-2023-QR-001). Computer Emergency Response Team-India. https://www.cert-in.org.in
2. Code of Criminal Procedure, 1973, § 357A (India).
3. Government of India. (2000). Information Technology Act, 2000 (as amended). India Code. https://www.indiacode.nic.in (Sections cited: 66C, 66D, 66E, 67, 67A, 67B, 67C, 69A, 70B, 79)
4. Government of India, Ministry of Home Affairs. (2003). Report of the Committee on Reforms of the Criminal Justice System (Malimath Committee Report).
5. Government of India. (2012/2019). Protection of Children from Sexual Offences Act, 2012 (as amended).
6. Government of India. (2023). Bharatiya Nyaya Sanhita, 2023 (BNS) – Official Gazette/PRS Bill text (for Sections 77–79; mapping to IPC 354C–D, 509; and defamation consolidation at Sec 356).
7. Government of India. (2023). Bharatiya Sakshya Adhiniyam, 2023 – Sec 63 (electronic records admissibility).
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3(2)(b) (India).
9. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

10. Lalita Kumari v. Government of Uttar Pradesh, (2014) 2 SCC 1 (India).
11. Ministry of Electronics & Information Technology (MeitY). (2023, April 6; 2022, October 28 updates). Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (consolidated). (Timelines: 24-hour removal for NCI/impersonation; 72-hour LEA assistance; SSMI obligations).
12. Ministry of Home Affairs (MHA). (2023). Citizen Financial Cyber Fraud Reporting & Management System (CFCFRMS) – Helpline number 1930 & National Cyber Crime Reporting Portal. https://cybercrime.gov.in
13. National Crime Records Bureau (NCRB). (2022). Crime in India 2022: Cyber crime statistics. Ministry of Home Affairs.
14. National Payments Corporation of India (NPCI). (2022, February). Safety tips on UPI transactions (Advisory). https://www.npci.org.in
15. Nipun Saxena v. Union of India, (2019) 2 SCC 703 (India).
16. Reserve Bank of India (RBI). (2017, July 6). Customer protection – Limiting liability of customers in unauthorized electronic banking transactions (Circular DBR.No.Leg.BC.78/09.07.005/2017-18). https://www.rbi.org.in
17. Reserve Bank of India (RBI). (2021, November 12). Reserve Bank-Integrated Ombudsman Scheme (RB-IOS), 2021. https://www.rbi.org.in
18. Reserve Bank of India (RBI). (2022). RBI Ombudsman Scheme – FAQs: Know your rights in financial fraud cases. https://www.rbi.org.in
19. Shreya Singhal v. Union of India, (2015) (India) (Struck down Sec 66A; read down Sec 79; upheld Sec 69A).
20. United Nations. (1985). Declaration of basic principles of justice for victims of crime and abuse of power.