



Swami Vivekananda Advanced Journal for Research and Studies

Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X

Pg. 300-307



Cyber Crime and Cyber Security in India: Special Reference to Cyber Crimes against Women and Children

Dr. Rajesh Mani Tripathi

LL. M, Ph. D

Assistant Professor

rajeshmanibhu@gmail.com

Accepted: 20/11/2023

Published: 23/11/2023

DOI: <http://doi.org/10.5281/zenodo.20688919>

Abstract

The expansion of digital life in India has converted communication, banking, education and intimacy into networked activities. It has also created a difficult field of gendered and child-directed harm: cyber-stalking, morphing, identity theft, sextortion, grooming, circulation of intimate images and child sexual abuse material. This paper examines cyber crime and cyber security in India with special reference to women and children in 2023. It argues that Indian cyber law cannot be read only as a technology statute; it is also a constitutional and criminal-law project concerned with dignity, privacy, bodily integrity and procedural fairness. The paper evaluates the Information Technology Act, 2000, the IPC/POCSO framework applicable in 2023, the evidentiary rules for electronic records, institutional initiatives such as I4C and the National Cyber Crime Reporting Portal, and the reforms necessary for victim-centric cyber security.

Keywords: Cybercrime; cyber security; women; children; India; Information Technology Act; POCSO; NCRB; digital evidence

1. Introduction

Cyber crime in India is no longer an exceptional category of computer misuse. It is part of ordinary social and economic life because the devices through which people learn, love, work, borrow, pay, travel and express themselves are also the devices through which offenders identify, profile and attack them. The National Crime Records Bureau, as reported by the Ministry of Home Affairs, records cyber-crime cases involving communication devices as medium or target and identifies 2023 as the latest published year for Crime in India data.¹ The point is not merely statistical. Cyber crime changes the grammar of victimisation: one image can be copied without exhaustion, a threat can cross several states in seconds, and a child can be approached without any visible entry into the house. For women and children, the harm is frequently reputational, sexualised, repetitive and socially amplified.

This paper therefore treats cyber security as a legal, institutional and social arrangement rather than a purely technical discipline. Firewalls, encryption and secure authentication are necessary, but they are insufficient when a school-going child is groomed in an online game, when a woman is blackmailed with a morphed photograph, or when a survivor is compelled to negotiate with police, platform, family and community shame at the same time. A rights-based approach asks three questions: what conduct is criminalised, how quickly can the harmful content or account be stopped, and whether the process protects rather than re-traumatises the victim. The paper uses 2023 as a focal year, while also noting subsequent institutional or statutory developments where they clarify the present position. It makes a modest but important claim: India's cyber-security law must move from event-based policing to continuing digital care.

The choice to focus on women and children is not a sentimental add-on to cyber law. Gender and age shape the form, gravity and aftermath of cyber offences. A fraudulent investment message harms any citizen, but an intimate image circulated without consent may affect a woman's marriage, employment, housing and physical safety. A phishing link sent to a child may be accompanied by grooming, secrecy and

emotional dependency. The Protection of Children from Sexual Offences Act, 2012 and the Information Technology Act, 2000 respond to some of these harms, yet the fragmented interface between criminal law, platform governance and digital evidence often leaves the victim to carry the burden of coordination.² That burden is too heavy. It explains why cyber-security policy has to be gender-sensitive, child-sensitive and procedurally simple.

2. Conceptualising Cyber Crime and Cyber Security

Cyber crime is usually defined by either the means or the object of the offence. In some cases the computer or mobile device is the target, as in unauthorised access, malware, denial-of-service attacks or damage to computer resources. In other cases the device is the medium, as in cheating by impersonation, cyber stalking, non-consensual circulation of sexual images, obscenity, child sexual abuse material, identity theft or extortion. The Information Technology Act, 2000 supplies the core statutory vocabulary by granting legal recognition to electronic records and by penalising specific forms of computer-related wrongdoing.³ But Indian cyber crime is not confined to that Act. In 2023 it was also prosecuted through the Indian Penal Code, 1860, the POCSO Act, 2012, the Indecent Representation of Women (Prohibition) Act, 1986, and procedural/evidentiary rules governing search, seizure and admissibility.

Cyber security, in contrast, is a preventive and resilience-oriented idea. It involves the capacity to identify risk, reduce vulnerability, respond to attacks and restore trust after harm. A narrow view would treat cyber security as the task of experts in computer emergency response. A wider constitutional view sees it as a public function because insecurity online can silence speech, restrict mobility, undermine equal citizenship and convert privacy into a privilege of those who can pay for protection. The wider view is especially necessary in relation to women and children. Victims often face victim-blaming and threats of exposure; consequently they may delete evidence, delay reporting or settle privately with offenders. Legal design must recognise this

¹ Press Information Bureau, Ministry of Home Affairs, "Cyber Crime Cases", March 17, 2026, available at: <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241339> (last visited on June 11, 2026).

² The Protection of Children from Sexual Offences Act, 2012, ss. 11, 13-15; Information Technology Act, 2000, ss. 66E, 67, 67A and 67B.

³ Information Technology Act, 2000, Act 21 of 2000, long title and ss. 43, 66, 66C, 66D, 66E, 67, 67A, 67B, 69A and 70B.

behavioural reality. The best cyber security system is not the one that speaks in the most technical language; it is the one that a frightened person can actually use at midnight.

India's constitutional jurisprudence supports this wider approach. The Supreme Court has affirmed privacy as intrinsic to life and personal liberty under Article 21, and privacy includes bodily privacy, decisional autonomy, informational control and the protection of intimate zones of life.⁴ Cyber crimes against women and children commonly violate all these dimensions at once. A deepfake pornographic clip is not merely obscene content; it is an attack on identity and autonomy. Online grooming is not merely communication; it is manipulation of vulnerability. The constitutional vocabulary of dignity and privacy therefore helps to interpret ordinary cyber offences in a manner that is attentive to the actual harm. It also insists that investigation must not become a second violation. Phones should not be casually searched, intimate evidence should not be circulated among officials, and protection must not be made conditional on the victim's social conformity.

3. Trends and the 2023 Moment

The 2023 data reveal the scale at which digital offences have become ordinary police business. The PIB annexure based on NCRB data shows all-India cyber-crime cases rising from 52,974 in 2021 to 65,893 in 2022 and to 86,420 in 2023.⁵ The increase is significant even before one considers under-reporting. Many victims do not report because they fear public disclosure, police insensitivity, family backlash or the futility of action against anonymous accounts. Women may be told to leave social media. Children may be scolded for using a phone rather than treated as victims of predation. Therefore, official numbers should be read as a floor, not as the whole field of harm. The rise also indicates better reporting and higher digital penetration, but the law should not hide behind that explanation. More reporting still means more legal workload, more forensic demand and a greater need for fast victim support.

State-wise data also show that cyber crime is not evenly distributed. Karnataka, Telangana, Uttar Pradesh and Maharashtra feature prominently in 2023 figures, while several smaller states report much lower

numbers.⁶ This distribution may reflect population, internet use, commercial activity, reporting capacity and policing infrastructure rather than the pure incidence of crime. It is unsafe to infer that a low-reporting state is necessarily a safe state. A woman in a district without a cyber cell may experience the same harm as a woman in Bengaluru, but only the latter may find a recognisable reporting channel. In child-related cases, the gap is even more sensitive because reporting depends on adult awareness. A child rarely walks into a police station to describe grooming. The law must therefore build detection, counselling and reporting pathways through schools, child welfare institutions and health systems, not only through police stations.

The 2023 moment is also marked by the convergence of older offences and newer tools. Stalking, obscenity, cheating, extortion and sexual harassment are not new. What is new is the affordance of scale, anonymity, speed, searchability and synthetic alteration. A morphed image that once required skill can now be produced using consumer apps. A fake investment website can look professional. A child can be persuaded to share personal images in a private chat, and then that private chat becomes a mechanism of continuing blackmail. Cyber security must therefore address ordinary social relations as much as sophisticated hacking. It is a mistake, sometimes made in policy discussion, to imagine cyber crime as a battle only between the state and a hacker. Much of the gendered harm is intimate, local, vindictive and repetitive. The offender may be a classmate, colleague, neighbour, former partner or a person using fake digital proximity.

4. Statutory Framework in 2023

The Information Technology Act, 2000 remains the principal technology statute. Section 43 deals with civil liability for unauthorised access, downloading, contamination by virus and similar damage. Section 66 converts several acts into criminal offences when done dishonestly or fraudulently. Sections 66C and 66D address identity theft and cheating by personation through computer resources. Section 66E punishes violation of privacy by capturing or transmitting images of a private area. Sections 67, 67A and 67B criminalise obscene material, sexually explicit material and child sexual abuse material in electronic

⁴ K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

⁵ Press Information Bureau, Ministry of Home Affairs, "Cyber Crime Cases", March 17, 2026, Annexure-I, available at:

<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241339> (last visited on June 11, 2026).

⁶ Ibid. The annexure reports, inter alia, Karnataka at 21,889 cases, Telangana at 18,236 cases, Uttar Pradesh at 10,794 cases and Maharashtra at 8,103 cases in 2023.

form. These provisions matter because many offences against women and children involve exactly such acts: impersonation, capture, transmission, storage, publication and coercive circulation. Yet the provisions are drafted in a largely content-and-access vocabulary, while modern harms may involve synthetic generation, algorithmic amplification and platform monetisation. The statute needs interpretation and updating, not casual abandonment.

In 2023 the Indian Penal Code, 1860 still supplied key offences such as stalking under section 354D, voyeurism under section 354C, outraging modesty, insult to modesty, cheating, criminal intimidation, extortion and defamation. The POCSO Act supplied a child-specific protective code, including sexual harassment, use of a child for pornographic purposes and possession/storage of child sexual abuse material. The overlap is not a drafting error; it reflects the layered nature of cyber harm. A single act of threatening a 15-year-old girl with a recorded video may attract POCSO, IT Act and IPC provisions. The challenge is not overlap as such, but poor charge selection and weak investigation. Officers must avoid both under-charging and indiscriminate over-charging. A precise charge-sheet improves the chances of conviction and reduces the scope for defence arguments about vagueness or procedural unfairness. This is where training becomes a due-process issue, not an administrative luxury.⁷

Electronic evidence is the hinge on which most cyber cases turn. Chat records, IP logs, subscriber information, device images, hash values, screenshots and server records must be collected and proved in a manner acceptable to court. The Supreme Court's decisions in *Anvar P.V.* and *Arjun Panditrao* emphasise the requirements for admissibility of electronic records under section 65B of the Indian Evidence Act, 1872.⁸ In practice, victims often bring screenshots; platforms hold logs; telecom companies hold subscriber details; and the device may belong to a family member. A cyber-security response must therefore include standard forms, preservation requests, chain-of-custody protocols and quick freezing of volatile data. An error at this stage can destroy an otherwise strong case. Many victims learn this too late, after messages are deleted or accounts vanish. Investigation must begin with preservation, not with moral questioning of the complainant.

5. Cyber Crimes against Women

Cyber crimes against women are frequently sexualised even when the original dispute is not sexual. Online abuse often uses rape threats, casteist or communal slurs, body shaming, threats of exposure, doxing and reputational attacks. Cyber-stalking may involve repeated messages, fake profiles, tracking, impersonation and monitoring of location or social connections. The law recognises stalking, voyeurism and violation of privacy, but enforcement often struggles because conduct occurs in fragments across platforms. One message may look minor; the pattern is terrifying. A woman may block an account, and the offender returns through another account. A good investigation therefore reconstructs the pattern rather than isolating a single abusive message. Courts and police should also treat reputational harm seriously. The fear of a morphed image being sent to relatives can control a woman's life as effectively as a physical threat. It can change how she dresses, travels, studies or speaks online.

Non-consensual intimate imagery and morphed sexual content create a particularly intense form of harm. The injury is not exhausted when the image is removed because the victim cannot know who saved it, where it may reappear, or whether future relationships and employment will be affected. This uncertainty produces a continuing injury. In 2023, widely available image-editing tools and the early mainstreaming of generative artificial intelligence made the problem worse. The law should not require the victim to prove physical capture if the image is synthetic; the wrong lies in the unauthorised sexual representation and circulation of identity. Indian law can already respond through privacy, obscenity, defamation, intimidation and harassment provisions, but the language of some provisions is not fully suited to deepfake harms. A clear offence for malicious synthetic sexual depiction would reduce uncertainty. Till then, investigators should not dismiss deepfake material as unreal. It is unreal in production but very real in consequences.

The Supreme Court's decision in *Shreya Singhal* remains relevant because it invalidated section 66A of the IT Act for overbreadth and protected online speech

⁷ Indian Penal Code, 1860, ss. 354C, 354D, 384, 499, 503 and 509; Protection of Children from Sexual Offences Act, 2012, ss. 11, 13-15.

⁸ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

from vague criminalisation.⁹ The case is sometimes misunderstood as a barrier to action against online abuse. It is not. It means that cyber law must be precise, proportionate and constitutionally disciplined. Women do not gain security from vague provisions that can also be used against complainants, journalists or dissenters. Nor do they gain security from a law that over-criminalises expression while under-enforcing actual threats and sexualised harm. The correct lesson is narrower: harmful conduct must be defined clearly; lawful speech must not be chilled; and takedown or blocking powers must be accompanied by procedural safeguards. A constitutional cyber-security model protects both freedom and safety. These are not opposite values, although public debate often acts as if they are.

6. Cyber Crimes against Children

Children experience cyber harm through dependency, curiosity and developmental vulnerability. Offenders exploit the desire for friendship, gaming rewards, attention, romance or fear of punishment. Grooming rarely begins with an explicit request. It may begin with ordinary conversation, gifts, secrecy and emotional isolation. By the time a child shares an image or agrees to meet, the child may feel responsible for the situation. Law must therefore avoid adult assumptions about consent and choice. POCSO's child-protective structure is crucial because it refuses to convert a child's apparent cooperation into legal consent. In cyber cases this principle becomes even more important, since the child may have typed messages, clicked links or continued conversation. Those acts should not obscure the offender's manipulation. Good investigation listens carefully, uses child-friendly procedures and avoids making the child narrate the incident repeatedly before multiple adults.

Section 67B of the IT Act is central to child sexual abuse material in electronic form. It covers publishing or transmitting material depicting children in sexually explicit acts, creating or collecting such material, browsing, downloading, advertising, exchanging or distributing in specified circumstances, and facilitating online abuse. The POCSO Act separately addresses use of children for pornographic purposes and aggravated situations. Together these provisions can respond to production, possession and circulation. Yet child-protection law increasingly faces

encrypted channels, offshore hosting and closed groups. Hash-matching, trusted flagging systems, prompt platform cooperation and cross-border mutual legal assistance become essential. The law must also distinguish between a child victim's coerced self-generated image and an adult offender's possession or circulation of it. Treating a child as an accused because an image originated from the child's phone would be a grave mistake. The legal system should prosecute exploitation, not adolescent vulnerability.¹⁰

A further difficulty is that many cyber risks for children are embedded in normal digital spaces: education apps, gaming platforms, messaging groups, short-video platforms and online payment systems. The household cannot supervise every interaction. Nor is blanket prohibition a sensible policy, because digital participation is increasingly connected with education and social inclusion. The appropriate framework is layered: age-appropriate design, strong reporting tools, parental literacy without surveillance panic, school counselling, platform moderation, and quick law-enforcement response for high-risk cases. Cyber security education should not merely say 'do not share OTP' or 'do not talk to strangers'. It must explain grooming, coercion, privacy settings, reporting, consent, and the difference between blame and responsibility. Children need a vocabulary to describe uncomfortable online experiences. Many childrens simply do not know that what happened has a legal name, and that ignorance protects the offender.

7. Institutional Architecture and Government Initiatives

India's institutional response has become more elaborate. The Indian Cyber Crime Coordination Centre (I4C), the National Cyber Crime Reporting Portal, cyber forensic-cum-training laboratories and financial assistance under the Cyber Crime Prevention against Women and Children scheme show recognition that ordinary police structures need specialised support. The Ministry of Home Affairs has stated that the National Cyber Crime Reporting Portal was launched to enable reporting of all types of cyber crime, with special focus on cyber crimes against women and children, and that assistance was provided to states and union territories for forensic and training

⁹ Shreya Singhal v. Union of India, AIR 2015 SC 1523; (2015) 5 SCC 1.

¹⁰ Information Technology Act, 2000, s. 67B; Protection of Children from Sexual Offences Act, 2012, ss. 13-15 and 24-27.

laboratories.¹¹ Such measures matter because cyber offences are time-sensitive. A delay in registration, preservation or platform request may make recovery impossible. Central coordination can also help identify patterns where the same accused or infrastructure affects victims in multiple states.

However, institutional expansion does not automatically produce victim-centric justice. A portal that is difficult to use, a helpline that gives generic advice, or a police station that treats online sexual harm as a family matter will fail in practice. The first response should be structured: record the complaint, advise preservation of evidence, assess immediate risk, initiate takedown or preservation requests, and offer referral to counselling or child welfare services. For women, the response must not demand unnecessary disclosure to family members. For children, it must involve child-friendly procedures and mandatory reporting norms without turning the home into a hostile interrogation site. Cyber-security institutions should publish clear service standards: expected timelines for acknowledgement, content preservation, platform escalation and referral. Law is often experienced as a queue. For a victim of intimate-image abuse, each hour of waiting is not neutral time; it is fresh injury.

Capacity building is not only a matter of more laboratories. Police, prosecutors, magistrates and legal-services authorities need shared training. A police officer may know how to receive a complaint but not how to frame a preservation request. A prosecutor may understand POCSO but not metadata. A magistrate may grant remand but not ask whether the victim's private data has been protected. Legal aid lawyers may advise settlement without appreciating long-term digital circulation. This is why cyber security should be understood as a chain. Its strength is determined by the weakest link. India has invested in the visible parts of the chain; the less visible parts, including counselling, witness protection, forensic documentation, public defenders, victim compensation and survivor privacy, require equal attention. Otherwise the system will receive complaints without delivering justice.

8. Challenges in Investigation, Adjudication and Platform Governance

Jurisdiction is a practical and doctrinal challenge. The offender, victim, server, payment account and platform may be located in different territories. Police stations may refuse registration by claiming lack of jurisdiction, even though cyber offences often produce consequences within the complainant's locality. A victim-centric rule should allow the complainant to report where she resides or where the harm is experienced, followed by transfer or coordination where necessary. Delay caused by jurisdictional debate benefits offenders. The Criminal Procedure Code in force during 2023 and the general principles of territorial jurisdiction can accommodate such an approach, but police practice needs clarity. There is also the problem of anonymity. Fake accounts, VPNs, mule accounts and stolen SIM cards complicate identification. Yet anonymity should not become an excuse for non-registration. Many cases are solved through payment trails, device forensics, recovery of login details, witness accounts or repeated behavioural patterns.

Platform governance raises a different set of concerns. Intermediaries are often the only actors able to remove harmful content quickly, preserve logs and prevent re-upload. At the same time, excessive private censorship can harm lawful expression and due process. The intermediary safe-harbour framework under section 79 of the IT Act and the due-diligence rules seeks to balance these concerns. For women and children, the urgent need is a specialised and accountable escalation pathway for sexualised abuse, child sexual abuse material, impersonation and threats. The platform should not require repeated reporting by the same victim for mirror uploads of the same image. Hash-based detection and trusted channels can reduce that burden, subject to safeguards against over-removal and misuse. The legal question is not whether platforms should act; they already govern speech privately. The question is how to make that governance transparent, accountable and rights-respecting.¹²

Adjudication presents still another difficulty: the courtroom may not understand the experience of online harm. Defence arguments sometimes trivialise cyber abuse because there is no physical contact. This approach is outdated. Digital injury can affect mental health, education, employment, social standing and physical safety. It may also trigger offline violence.

¹¹ Press Information Bureau, Ministry of Home Affairs, "Increase in Cyber Crimes", February 7, 2024, available at: <https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505> (last visited on June 11, 2026).

¹² Information Technology Act, 2000, s. 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

Courts should recognise continuing harm when bail conditions, protection orders and compensation are considered. At the same time, criminal procedure must remain fair. Accused persons are entitled to disclosure, cross-examination and protection against unreliable electronic evidence. A victim-centric system is not an anti-accused system. It is a system that avoids unnecessary humiliation of the complainant while insisting on rigorous proof. The two commitments can co-exist, though it requires judicial discipline.

9. Towards Victim-Centric Cyber Security

A victim-centric model begins before the offence. Digital literacy campaigns must move beyond slogans. Users should know how to enable two-factor authentication, control privacy settings, recognise phishing and preserve evidence. Women and girls should not be told that the solution is withdrawal from online space. Safety advice that restricts women's public participation reproduces the same inequality that cyber abuse seeks to enforce. The better message is: participate, secure accounts, document abuse, report early and demand institutional help. For children, cyber education should be age-graded and practical. It should teach that a trusted online friend can still be unsafe, that threats of exposure are a tactic, and that asking for help will not automatically result in punishment. Such education is a form of legal empowerment.

The second element is design. Platforms, schools, banks and public agencies should build safety into systems. Default privacy for minors, friction for forwarding intimate material, rapid account recovery, warning labels for suspicious links, easy reporting of impersonation, and clear audit trails can prevent harm. Cyber security should not depend entirely on user caution. The user is frequently tired, young, frightened or misled. Design must anticipate human behaviour, including mistakes. This is particularly important in India, where first-generation internet users may not be fluent in English or legal language. Reporting tools must be multilingual, simple and available on mobile devices. The forms should not ask irrelevant questions. A small interface decision can determine whether a victim completes the complaint or abandons it halfway.

The third element is legal reform. India needs clearer recognition of non-consensual intimate imagery, synthetic sexual depictions, cyber-flashing and coordinated online harassment. It also needs better integration of cyber offences with victim compensation and counselling. The new Bharatiya

Nyaya Sanhita, 2023, which came into force after the focal year, reorganises offences relating to women and children; yet statutory reorganisation alone cannot solve implementation deficits. Reforms should include model investigation protocols, mandatory evidence-preservation checklists, privacy-protective handling of devices, special training for prosecutors and judges, and measurable timelines for platform cooperation. The law must also deal with cross-border data requests more efficiently. Mutual legal assistance that takes months is unsuitable for content that spreads within minutes. India should pursue lawful, rights-based channels for expedited preservation and disclosure in serious sexual and child-protection cases.

Finally, cyber security must include aftercare. The victim may need counselling, school support, workplace accommodation, relocation advice, identity-document protection or help in removing repeated uploads. The legal system often treats registration of FIR as the main event. For the victim, it may be only the beginning. A woman whose morphed image is repeatedly uploaded may require months of monitoring and legal support. A child victim may need therapeutic intervention to address shame and fear. Compensation should recognise digital harm even where there is no physical injury. Community education is also necessary to reduce stigma. The social life of a cyber offence is shaped by the people who share, laugh, threaten or remain silent. Criminal law can punish the core offender, but prevention requires changing bystander behaviour too.

10. Conclusion

Cyber crime and cyber security in India must be understood as questions of constitutional citizenship. In 2023, the scale of cyber-crime reporting and the nature of offences against women and children showed that digital harm is not peripheral to criminal justice. It is central to dignity, privacy, equality and access to public life. The existing legal framework provides several useful tools: the IT Act, IPC provisions applicable in 2023, POCSO, electronic evidence rules, intermediary regulation and specialised reporting mechanisms. But the system still suffers from fragmentation, delays, weak forensic capacity, uneven police sensitivity and insufficient aftercare. Women and children require a response that is quick, respectful, technically competent and legally precise.

The best way forward is not to choose between technology and law, or between free speech and safety. India needs a layered model: precise offences, constitutional safeguards, strong forensic practice,

accountable platforms, child-friendly and gender-sensitive procedures, legal aid, counselling and public education. Cyber security should be measured not only by the number of portals or laboratories but by the experience of the person who reports harm. Did the system believe her? Did it protect the child? Did it preserve evidence? Did it remove content quickly? Did it prevent repetition? These questions should guide the next stage of Indian cyber law. A secure digital India will be achieved not by fear of the internet, but by making rights enforceable in the spaces where life now actually occurs.

Bibliography

Information Technology Act, 2000, Act 21 of 2000.
 Protection of Children from Sexual Offences Act, 2012, Act 32 of 2012.
 Indian Penal Code, 1860, Act 45 of 1860.
 National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India).

Press Information Bureau, Ministry of Home Affairs, "Cyber Crime Cases", March 17, 2026.

K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

Shreya Singhal v. Union of India, AIR 2015 SC 1523.

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.

Disclaimer/Publisher's Note: The views, findings, conclusions, and opinions expressed in articles published in this journal are exclusively those of the individual author(s) and contributor(s). The publisher and/or editorial team neither endorse nor necessarily share these viewpoints. The publisher and/or editors assume no responsibility or liability for any damage, harm, loss, or injury, whether personal or otherwise, that might occur from the use, interpretation, or reliance upon the information, methods, instructions, or products discussed in the journal's content.
