AI, GENDER AND DIGITAL JUSTICE: INVESTIGATING THE MISUSE OF INFORMATION TECHNOLOGY ACT BY WOMEN IN INDIA

Pankaj[1], Dr. Reetika Bansal[2], Dr. Puja Jaiswal[3], Dr. Manjinder Gulyani[4], Dr. Meenakshi Sharma[5], Rupali Sharma[6]

[1]Ph.D Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana Ambala, Haryana, India,
[2]Professor, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana Ambala, Haryana, India,
[3]Head of Department and Associate Professor, Dr. B.R. Ambedkar National Law University, Sonipat, Haryana, India,
[4]Associate Professor, Institute of Law, Kurukshetra University, Kurukshetra, Haryana, India,
[5]Assistant Professor, Chandigarh Group of Colleges Jhanjeri, Mohali, Panjab, India, [6]Assistant Professor, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana Ambala, Haryana, India,

pankajadv.79@gmail.com[1]
bansalreetika80@gmail.com[2]
jais.puja@gmail.com[3]
77manjinder@gmail.com[4]
Meenakshi01984@gmail.com[5]
rupalisharma7828@gmail.com[6]

Abstract

In today's digital age, the intersection of artificial intelligence (AI), gender, and justice has created new opportunities for empowerment but also new forms of misuse. India's Information Technology Act, 2000 was originally designed to protect individuals, especially women, from online abuse, cyberstalking, and digital exploitation. Yet, recent developments show a troubling trend: the same law that was meant to protect is, at times, being misused by women to make false or exaggerated cyber complaints, often as a tool for personal revenge or social leverage.

This research explores how the IT Act, particularly its key sections on cyber offences and obscenity, has been used and misused in gendered contexts. It looks closely at how digital evidence, social media, and AI based technologies play a role in both proving and fabricating such cases. Through a blend of legal analysis, real life case studies, and insights from AI ethics and gender theory, the paper examines the fine line between justice and manipulation in the digital space.

By unpacking this complex issue, the study seeks to highlight the need for balance—a justice system that continues to protect women from genuine harm while preventing the misuse of cyber laws. It also emphasizes the role of AI transparency, digital literacy, and fair investigation processes to ensure that technology remains a tool for truth, not for distortion. Ultimately, the research aims to contribute to a more equitable and accountable digital justice framework for India, one that truly serves both gender justice and technological integrity.

Keywords: Artificial Intelligence (AI); Gender Justice; Digital Justice; Information Technology Act, 2000; Cybercrime; Misuse of Law; Women and Technology; Cyber Harassment; Digital Ethics; Algorithmic Bias; False Cyber Complaints; Feminist Jurisprudence; Digital Evidence; Legal Accountability; Online Defamation; Technological Misuse in Gender Contexts; AI in Law Enforcement; Cyber Law Reform; Digital Literacy; India.

Introduction

The digital revolution has fundamentally transformed how people communicate, work, and seek justice. In India, the increasing use of technology has brought both empowerment and vulnerability, particularly in the context of gender relations. The Information Technology Act, 2000 (IT Act) was introduced as a progressive legal framework to regulate online activities, ensure data security, and curb cybercrimes such as harassment, stalking, defamation, and the circulation of obscene material. For many women, it has become a critical tool to report online abuse and safeguard their digital dignity. However, with the growing dependence on digital platforms and the complexities of online interactions, a parallel concern has emerged — the misuse of the same legal protections intended to ensure justice.

In recent years, reports and case studies have shown instances where provisions of the IT Act have been strategically misused by women to file false or exaggerated complaints, often as a means of personal retaliation or reputation management. Such misuse not only undermines the credibility of genuine victims but also places an additional burden on law enforcement and the judiciary. This trend calls for a deeper understanding of the social, legal, and technological dimensions of gendered digital justice.

Simultaneously, the rise of artificial intelligence (AI) in the legal and justice ecosystem has introduced new tools for digital surveillance, evidence verification, and predictive policing. While AI technologies hold immense potential for promoting fairness and efficiency, they also raise critical concerns about algorithmic bias, privacy intrusion, and ethical accountability. When gender dynamics and technology intersect, the outcomes can either enhance justice or distort it. The integration of AI in digital evidence assessment, for example, may help identify patterns of cyber abuse, but it can also be manipulated or misinterpreted in cases of fabricated digital proof.

This paper investigates the dual nature of digital justice in India—how the IT Act, when intersecting with gendered social structures and emerging AI technologies, can both empower and be exploited. It seeks to examine the legal framework governing cyber offences through a gender sensitive lens, assess the role of AI in detecting misuse, and explore the ethical dilemmas arising from such interactions. By analyzing statutory provisions, judicial precedents, and real life case examples, the research aims to uncover how the misuse of cyber laws by women challenges the very principles of justice they were designed to uphold.

Ultimately, this study advocates for a balanced and reform oriented digital justice system, one that recognizes women's rights to online safety while ensuring procedural fairness for all. It calls for responsible AI integration, digital literacy programs, and transparent legal mechanisms that can safeguard against both cyber exploitation and legal manipulation. In doing so, the paper contributes to the ongoing discourse on gender, technology, and justice in the age of artificial intelligence, emphasizing that true equality in the digital era can only be achieved through accountability, empathy, and ethical innovation.

The Information Technology Act, 2000 (IT Act) stands as India's main legislation governing online conduct, cybersecurity, and digital communication. While its primary goal was to promote e governance and regulate cyber activities, several provisions have become crucial in addressing crimes that affect women disproportionately in online spaces.

One of the most debated provisions was Section 66A, which criminalized sending "offensive" or "menacing" messages through digital communication. Although originally meant to curb online harassment and protect women from abuse, it was often misused because of its vague and subjective language. The Supreme Court, in the landmark case *Shreya Singhal v. Union of India* (2015), struck it down for violating the right to free speech under Article 19(1)(a) of the Constitution. The judgment was a milestone, reaffirming that laws meant to protect should not silence legitimate expression.

Section 66D deals with cheating by personation using computer resources. This has been particularly important in cases involving fake social media profiles, impersonation, and identity theft all common forms of online exploitation faced by women. Likewise, Sections 67 and 67A penalize the publication or transmission of obscene and sexually explicit content in electronic form. These provisions have become critical in tackling crimes like revenge porn, circulation of morphed images, and sexual harassment through digital means.

Section 69 empowers government agencies to intercept, monitor, or decrypt information for security and investigative purposes. While this helps in tracing cyber offenders, it also raises privacy concerns, especially in cases involving women's personal communications. Finally, Section 72 addresses the breach of confidentiality and privacy, punishing anyone who discloses personal data obtained through official duties without consent. Together, these sections form the backbone of India's response to gendered cyber offences, offering protection — yet also demanding responsible enforcement.

Protection of Women under the IT Act: Genuine Safeguards for Online Harassment, Defamation, and Obscenity

The IT Act has played a crucial role in helping women seek justice in the digital realm. As online spaces increasingly blur with personal and professional lives, women face unique forms of abuse from cyberstalking and trolling to the non consensual sharing of private images. Sections 66D, 67, and 67A have provided legal tools to report such acts and demand accountability. For many women, these provisions represent a form of empowerment an assurance that the law recognizes digital abuse as seriously as physical harm.

The creation of cybercrime reporting portals and dedicated cyber cells has also made justice more accessible. Platforms like the *National Cyber Crime Reporting Portal* allow victims to file complaints from the safety of their homes, often with anonymity. Moreover, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 strengthened these protections by placing greater responsibility on social media platforms to remove harmful or obscene content swiftly.

These safeguards have brought meaningful progress toward digital gender equality, ensuring that women are not forced to withdraw from online spaces out of fear. Yet, as with many protective laws, the possibility of misuse or overreach persists. In some cases, the same provisions have been turned into tools for personal retaliation or social leverage, revealing a delicate tension between protection and accountability in India's digital justice framework.

Courts in India have played a vital role in defining how the IT Act applies in gender sensitive contexts. Through their judgments, they have tried to balance the right to protection with the right to free expression and fair process.

In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A, holding that its vague terms like "offensive" and "annoying" gave authorities unrestricted power to curb speech, including women's online expression. The judgment emphasized that safeguarding dignity should not come at the cost of fundamental freedoms.

Earlier, in *State of Tamil Nadu v. Suhas Katti* (2004), one of the first cybercrime convictions in India, a man was punished under Sections 67 and 67A for posting obscene material and harassing a woman online. The case demonstrated how the IT Act could effectively serve victims of digital abuse. Similarly, in *Aveek Sarkar v. State of West Bengal* (2014), the Supreme Court clarified that obscenity must be judged using contemporary community standards, preventing moral policing of women's online presence.

However, in cases like *Mahesh Bhatt v. Union of India* (2020), the Court acknowledged the dangers of overreach and frivolous complaints, emphasizing that the law must protect both dignity and due process. Together, these decisions underscore the judiciary's evolving effort to balance empowerment with fairness in India's digital era.

Real life cases offer a deeper look into how the IT Act functions and sometimes falters in practice. In many instances, women have used the law to reclaim agency and justice. For example, victims of revenge pornography or online blackmail have successfully used Sections 66E, 67, and 67A to ensure offenders are held accountable. These victories not only deliver justice to individuals but also signal a strong message against the normalization of digital violence.

Yet, alongside genuine cases, there have been incidents of false accusations and fabricated evidence, where the law has been exploited for personal gain. Some complaints have relied on edited screenshots, fake messages, or manipulated images, leading to wrongful arrests and public humiliation of innocent individuals. Such instances harm the integrity of the justice system and erode trust in women's digital rights movements.

In today's era of rapid information sharing, even a single false claim can spread widely through social media, turning into digital character assassination. This underscores a fundamental challenge for law enforcement how to protect victims without enabling misuse. The solution lies not in weakening legal protections for women, but in strengthening digital forensics, AI assisted evidence verification, and gender neutral investigation protocols. Only then can the IT Act truly fulfill its purpose: to ensure justice rooted in truth, dignity, and equality.

Misuse of the IT Act by Women: A Critical Examination

The Information Technology Act, 2000 was designed as a protective legal shield especially for vulnerable users navigating the fast changing world of digital communication. For many women, it has become a vital means to report harassment, stalking, and online defamation, helping them reclaim safety and dignity in virtual spaces. However, just as any powerful law can be misapplied, the IT Act too has seen instances where its provisions have been used with questionable intent. Misuse, in this context, does not mean that women should not have strong digital rights, but that false or exaggerated claims under the guise of victimhood can distort justice and harm genuine causes.

Legally, misuse occurs when individuals manipulate digital evidence, fabricate social media interactions, or lodge frivolous complaints to settle personal scores be it in domestic disputes, workplace rivalries, or social conflicts. Ethically, such actions blur the line between empowerment and exploitation of the legal system. The challenge lies in maintaining faith in gender justice frameworks while ensuring that laws are not wielded as instruments of revenge or coercion. Thus, understanding misuse requires a careful balance between empathy for victims and accountability for those who deliberately misuse the law.

In recent years, cybercrime units and legal practitioners have observed recurring patterns of misuse involving women complainants. A frequent example includes false claims of cyberstalking or online defamation, often based on selective screenshots or out of context messages. In some cases, women have been found to create fake profiles or alter chat histories to fabricate narratives of harassment. There have also been reports of revenge driven complaints against former partners or colleagues, leveraging the fear of arrest and social stigma that comes with being accused of a “cyber offence.”

Such misuse not only damages reputations but also diverts investigative resources away from genuine victims who need timely intervention. Moreover, as digital evidence can be easily manipulated, distinguishing truth from fabrication becomes increasingly difficult for authorities. The lack of digital literacy among investigators, combined with public sympathy toward women complainants, often leads to premature assumptions of guilt. These patterns highlight the urgent need for objective evidence verification mechanisms and AI based digital forensics that can authenticate electronic data before prosecution.

When legal provisions intended for protection are misused, the very notion of justice becomes distorted. Men who are falsely accused under the IT Act often face public shaming, reputational damage, and emotional distress long before the truth is established. The social presumption of female victimhood in cyber contexts can further complicate matters, as law enforcement agencies may act hastily out of perceived moral duty rather than evidentiary balance.

Such misuse also undermines the credibility of genuine female victims, creating skepticism in the justice system and the public sphere. Every false claim chips away at the trust built around women's safety in cyberspace. In a society already struggling with gender biases, misuse of digital laws risks reinforcing the stereotype that women "play the victim card," which can be deeply harmful to the broader movement for equality and digital justice. Therefore, both male and female experiences must be treated with procedural fairness, ensuring that justice remains impartial and evidence driven, not gender driven.

Media and Public Perception: The Gender Narrative Online

Media plays a powerful role in shaping how society perceives cyber offences involving gender. News headlines often sensationalize such cases, portraying women exclusively as victims and men as perpetrators, even before investigations conclude. This one dimensional narrative can amplify social biases and create moral panic around digital offences. While advocacy for women's safety online is essential, the tendency to overlook false or manipulative claims prevents an honest conversation about the complex realities of digital gender dynamics.

Social media platforms further magnify this imbalance. Viral posts, online "naming and shaming," and public campaigns can deliver instant judgment without due process. In such an environment, digital justice can easily turn into digital mob justice. Hence, responsible media reporting, coupled with public digital literacy, is crucial for ensuring that both protection and accountability coexist within India's online legal ecosystem.

The Role of Social Media in Amplifying Gendered Misuse

Social media platforms, while offering spaces for expression and activism, also act as accelerators of conflict and misinformation. In cases of alleged cyber harassment, platforms like Instagram, X (formerly Twitter), and Facebook often become battlegrounds where personal disputes are aired publicly. The ability to instantly post, share, and trend accusations gives complainants genuine or otherwise immense power to influence public opinion.

AI driven algorithms that prioritize engagement over accuracy further amplify emotionally charged content, allowing misinformation to spread rapidly. As a result, reputations can be destroyed overnight, long before facts are verified. This phenomenon highlights the double edged nature of digital empowerment: while women's voices have rightly found strength through online platforms, the absence of accountability mechanisms has created room for digital vigilantism. Ensuring fairness in such cases requires collaborative action from platform moderation and AI fact checking tools to stronger guidelines on responsible online conduct.

In essence, the misuse of the IT Act by women though not widespread represents a critical challenge for digital justice in India. It underscores the need to rethink how gender, law, and technology intersect in the 21st century. The goal should not be to silence women's voices but to ensure that the pursuit of justice remains grounded in truth, evidence, and equality. Only then can India's cyber laws truly serve their purpose: protecting the innocent, empowering the vulnerable, and upholding the integrity of digital justice.

Artificial Intelligence and Digital Justice

The emergence of Artificial Intelligence (AI) has brought a transformative shift in how justice systems function, particularly in the realm of cybercrime investigation and digital evidence management. In India, where the cyber landscape is rapidly expanding, AI technologies are increasingly being explored to support law enforcement agencies in tackling crimes under the Information Technology Act, 2000. However, this integration of AI into the justice process raises both opportunities and ethical dilemmas especially when viewed through the lens of gender and digital fairness.

AI has the potential to revolutionize cybercrime detection by enhancing the speed, precision, and scope of investigations. Law enforcement agencies are beginning to rely on facial recognition systems, data mining tools, and predictive policing algorithms to identify suspects, track digital footprints, and forecast criminal behavior. For instance, large datasets collected from social media, CCTV networks, and online platforms can be analyzed by AI to detect patterns of online harassment, identity theft, or financial fraud.

While these technologies promise efficiency, they also raise concerns about privacy violations and potential misuse. Without adequate safeguards, predictive policing could reinforce gender or social biases, targeting individuals or groups unfairly. The challenge, therefore, lies in developing AI assisted tools that enhance investigation without compromising human rights or perpetuating systemic prejudice.

One of the most promising uses of AI in digital justice is its ability to verify and authenticate electronic evidence. In an age where deepfakes, doctored screenshots, and synthetic audio or video content can easily be created, AI algorithms are being trained to identify traces of manipulation invisible to the human eye. These technologies analyze metadata, compression patterns, and digital fingerprints to determine whether an electronic record has been tampered with.

In gender based cybercrime cases such as morphing, revenge porn, or fabricated online defamation AI can play a decisive role in distinguishing between genuine evidence and falsified material. However, as with all technology, AI tools must be transparent and scientifically validated to ensure that they are not misused to fabricate evidence or misinterpret innocent data. The credibility of digital evidence thus depends not only on the sophistication of AI tools but also on the integrity and impartiality of the people using them.

Despite its promise, AI is not inherently neutral. Algorithms are trained on human data, and therefore often reflect human biases. When datasets carry implicit gender stereotypes or lack diverse representation, the resulting AI systems can produce discriminatory outcomes. For instance, sentiment analysis tools might misinterpret a woman’s emotional expression as aggression or manipulation; predictive policing algorithms might unfairly flag certain gendered behaviors as suspicious.

These biases pose a serious challenge to digital justice, especially when AI generated insights are used in criminal investigations or court proceedings. Without conscious efforts to audit and correct these biases, AI could unintentionally reinforce the same inequalities the law seeks to eliminate. A gender sensitive approach to AI design involving diverse programmers, ethical oversight, and algorithmic transparency is therefore essential to ensure fairness.

AI driven justice systems raise complex questions about privacy, consent, and accountability. The use of AI surveillance tools, biometric recognition, and automated data profiling can intrude deeply into individuals’ personal lives, especially women who are often victims of online stalking or image based abuse. Without informed consent and strict data protection norms, such interventions may end up violating the very privacy they claim to defend.

Moreover, when AI systems make errors such as wrongly identifying a suspect or misinterpreting evidence determining who is accountable becomes difficult. Is it the programmer, the police officer, or the algorithm itself? These ethical dilemmas highlight the urgent need for clear governance frameworks, ensuring that AI remains a tool for justice, not a replacement for human judgment. Accountability mechanisms must be built into every stage from data collection to decision making to maintain public trust.

For AI to truly serve the cause of digital justice, it must be designed around principles of fairness, transparency, and human oversight. AI should not replace the human element of empathy and reasoning but should assist judges, investigators, and policymakers in making more informed, unbiased decisions. Integrating AI responsibly can reduce delays in cybercrime trials, strengthen the evidentiary process, and help law enforcement differentiate between genuine and malicious complaints under the IT Act.

Further, the development of AI ethics charters, gender sensitive coding standards, and public accountability frameworks can ensure that technological innovation aligns with constitutional values of equality and due process. If used wisely, AI can act as a balancing force protecting women from real online harm while also preventing the misuse of cyber laws. The goal is not to create an automated justice system but to build a digitally intelligent one where technology amplifies fairness, not prejudice.

The evolving landscape of digital justice in India reflects a deep and ongoing tension between protecting women's rights online and preventing misuse of legal provisions under the *Information Technology Act, 2000*. The IT Act, while pioneering in its scope, is also a mirror of societal dynamics revealing how technology, law, and gender power relations interact. Artificial Intelligence (AI) now adds another layer to this complex web by influencing how justice is perceived, pursued, and delivered. This section synthesizes these themes, offering a holistic view of the gendered, legal, and ethical challenges of digital justice in India.

Balancing Gender Protection and Legal Misuse

Digital spaces have opened new avenues for empowerment but have also exposed women to unprecedented risks from cyberstalking and image based abuse to doxxing and online defamation. The Information Technology Act, 2000, particularly Sections 66D, 67, 67A, and 72, was instrumental in addressing these crimes. However, growing evidence suggests instances where the same legal protections have been strategically or emotionally misused, often in interpersonal or reputational disputes.

This dual reality poses a profound challenge: how can the legal system protect without overreaching, and believe without bias? A balanced approach must acknowledge that while women remain disproportionately targeted online, the misuse of protective laws can erode public faith in digital justice mechanisms. Ensuring due process, fair investigation, and proportional penalties is therefore critical. The aim should not be to question the credibility of women complainants, but to ensure that the law maintains truth as its ultimate measure of justice for both victims and the falsely accused.

Role of AI in Detecting Misuse while Safeguarding Rights

Artificial Intelligence, when applied ethically, can become a powerful ally in maintaining this balance. AI based tools can analyze patterns in cyber complaints, verify digital evidence authenticity, and detect inconsistencies that might indicate fabricated or exaggerated claims. For example, machine learning algorithms can identify whether an image or chat record has been altered, while natural language processing can detect malicious patterns in digital communication.

However, this promise comes with caution. Over reliance on automated systems risks turning justice into an algorithmic exercise devoid of human context. AI must function as a supporting mechanism, guided by ethical oversight and human review. The challenge lies in building systems that can detect misuse without undermining genuine victims. When designed with transparency and accountability, AI can act as a mediator between fairness and protection, reinforcing the integrity of India's digital justice framework.

The Indian judiciary has played a crucial role in defining the contours of cyber law, most notably through cases such as *Shreya Singhal v. Union of India (2015)*, which struck down Section 66A for its chilling effect on free speech. Yet, while courts have addressed misuse of law in principle, there remains no specific policy or statutory mechanism to address false or malicious cyber complaints. Many investigations continue without robust digital verification, leading to prolonged trials and reputational damage for the accused.

The absence of clear procedural safeguards for assessing electronic evidence authenticity or intent has widened the gap between technology and justice. Judicial pronouncements often emphasize protecting women, but they seldom address the need for balanced remedies when protection mechanisms are exploited. What India’s cyber jurisprudence requires is a gender neutral procedural framework one that safeguards genuine victims while also providing recourse against wrongful accusations, maintaining the integrity of justice in both directions.

Comparative Perspective: Insights from Other Jurisdictions on Gender and Digital Law Misuse

Globally, other jurisdictions have faced similar dilemmas. In the United Kingdom, the *Malicious Communications Act, 1988* and *Online Safety Act, 2023* distinguish between legitimate harassment claims and false allegations, emphasizing evidence based assessment and intent verification. The United States, under its *Computer Fraud and Abuse Act (CFAA)*, employs a tiered approach that categorizes digital misconduct by severity, ensuring proportional punishment. Meanwhile, the European Union’s GDPR framework emphasizes informed consent, accountability, and the right to redress for both victims and falsely accused individuals.

These international models offer valuable insights for India. They show that gender sensitive protection and anti misuse safeguards need not be contradictory — rather, they can coexist within transparent, data driven, and ethically monitored systems. Incorporating lessons from these jurisdictions could help India develop balanced cyber legislation that protects women without enabling systemic misuse.

At its core, the pursuit of digital justice is not merely a legal challenge but a moral and ethical project. The integration of AI and cyber laws must be guided by principles of fairness, accountability, and human dignity. As technology increasingly mediates the legal process from evidence gathering to predictive policing questions of bias, consent, and autonomy become central.

Ethically, justice in the digital era must transcend punitive responses and aim to restore trust in technology and law. Policy frameworks should encourage public awareness, digital literacy, and responsible online behavior, while simultaneously establishing independent oversight bodies to review AI assisted decisions. The ultimate goal should be to build a digital justice ecosystem where technology amplifies empathy, law ensures equality, and human judgment remains at the heart of every decision.

In sum, this discussion underscores that the future of digital justice in India depends on achieving harmony between protection and accountability, innovation and ethics, and law and humanity. These reflections naturally lead to the concluding argument: the need for a balanced, inclusive, and technologically aware justice framework that serves both women’s safety and systemic fairness.

Conclusion

The rapid digitization of society has transformed not only the way individuals communicate but also how justice is sought, delivered, and experienced. The Information Technology Act, 2000, as India’s foundational cyber law, was designed to protect citizens from the perils of online crime while enabling trust in the digital ecosystem. Over time, it has played a vital role in empowering women, offering them legal recourse against online harassment, cyberstalking, privacy violations, and obscenity. Yet, as this study has revealed, the same framework has also given rise to a complex and sensitive issue the misuse of legal protections, sometimes by women themselves, in ways that challenge both the spirit and structure of justice.

This paradox reflects a deeper truth: laws are human instruments, and their effectiveness depends not merely on what is written, but on how they are used. The misuse of the IT Act, whether intentional or inadvertent, does not undermine the need for protection but highlights the necessity of balance, integrity, and due process. Legal empowerment must always be accompanied by responsibility. Ensuring this balance is critical not only for gender justice but for maintaining the credibility of India’s digital legal system.

Artificial Intelligence (AI) offers a new dimension to this challenge. When applied ethically, AI can become a transformative force in the administration of justice verifying evidence, identifying manipulation, and streamlining cybercrime investigations. However, when applied without accountability, AI can also replicate existing biases and threaten privacy and autonomy. The future of digital justice therefore lies in human-centered AI, designed with transparency, empathy, and fairness. Technology should aid judgment, not replace it.

The research also underscores the pressing need for policy reform and education. Strengthening the IT Act through clearer definitions, procedural safeguards, and oversight mechanisms can reduce both misuse and victimization. Simultaneously, digital literacy programs, gender-sensitivity training, and ethical AI governance can nurture a culture of informed and responsible digital citizenship. These reforms must be complemented by balanced media reporting and public awareness efforts that promote fairness rather than polarization in cases involving gender and technology.

Ultimately, digital justice is not merely a legal pursuit it is a moral one. It calls for empathy as much as efficiency, fairness as much as enforcement. A gender-sensitive but gender-neutral justice system must evolve one that protects women from genuine harm while also guarding against the exploitation of legal safeguards. The Information Technology Act, guided by responsible human judgment and assisted by ethical AI, has the potential to embody this vision. In the coming years, India's journey toward digital justice will depend on how well it integrates law, technology, and humanity. A just digital society is not built through legislation alone but through collective awareness, ethical governance, and a shared commitment to truth. As we stand at the crossroads of gender, AI, and law, the path forward must be guided by one enduring principle: justice in the digital age must remain human at its core.

References

1) Agrawal, K. (2020). *Gendered Dimensions of Cyber Law: Understanding the IT Act and Its Impact on Women.* Journal of Indian Law & Technology, 16(2), 123–145.
2) Bansal, S. (2021). *Misuse of Cyber Laws: A Critical Analysis of IT Act Provisions in India.* Indian Journal of Criminology, 49(3), 211–229.
3) Basu, S. (2019). *Cyber Crime against Women: Legal Safeguards and Judicial Trends in India.* International Journal of Cyber Criminology, 13(1), 45–62.
4) Chaturvedi, R. (2022). *Artificial Intelligence in Justice Delivery: Challenges of Ethics and Accountability.* Indian Journal of Law & Technology, 18(1), 77–99.
5) Gill, L. (2021). *Digital Justice and Gender: Emerging Challenges in Indian Cyber Jurisprudence.* South Asian Law Review, 9(2), 66–88.
6) Mathur, A. (2020). *AI and Algorithmic Bias: Gender Justice in the Age of Automation.* Technology and Society Review, 12(4), 145–162.
7) NITI Aayog. (2021). *Responsible AI for All: Strategy for India.* Government of India. Retrieved from https://www.niti.gov.in.
8) Ministry of Electronics and Information Technology (MeitY). (2022). *National Cyber Security Policy (Draft).* Government of India.
9) United Nations Human Rights Council. (2021). *The Right to Privacy in the Digital Age: Gendered Perspectives.* A/HRC/47/24.
10) Srikrishna Committee Report. (2018). *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians.* Ministry of Electronics and Information Technology, Government of India.
11) *Supreme Court clarifies law on admissibility of electronic evidence without certificate under Section 65B.* (2020, July 14). SCC Online Blog. Retrieved from https://www.scconline.com/blog/post/2020/07/14/sc-clarifies-law-on-admissibility-of-electronic-evidence.

12) *Electronic Evidence and Gender Justice: Emerging Concerns in Cyber Jurisprudence.* (2021, June 7). SCC Online Blog. Retrieved from https://www.scconline.com/blog/post/2021/06/07/electronic-evidence-2.

13) *Hybrid System of Hearings.* (2023). E-Committee, Supreme Court of India. Retrieved from https://ecommitteesci.gov.in/project/hybrid-system-of-hearings/.

14) *Digitization of Records Project.* (2023). Department of Justice, Government of India. Retrieved from https://doj.gov.in/digitization-of-records/.

15) *Cyber Crime Investigation Manual.* (2023). Bureau of Police Research and Development, Ministry of Home Affairs, Government of India.

16) European Commission. (2022). *Artificial Intelligence Act (Proposal): Fostering Trust in AI.* Brussels: EU Publications.

17) OECD. (2021). *Recommendation on Artificial Intelligence.* Organisation for Economic Co-operation and Development.

18) UN Women. (2023). *Technology-Facilitated Gender-Based Violence: Global Policy Responses.* United Nations Publications.

19) Pew Research Center. (2021). *Gender, Technology, and Digital Harassment: Global Insights.* Retrieved from https://www.pewresearch.org.

20) World Bank. (2020). *E-Governance and Digital Inclusion: Building Gender-Sensitive Policy Frameworks.* World Bank Policy Report.