Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2026 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Digital Policing and Gendered Risks: Feminist Perspectives on Digital Policing, Rights, and Accountability in India

Smiksha[a]

[a]Chandigarh University, Mohali, India

Received 26 September 2026; *Accepted* 26 October 2026; *Published* 30 October 2026

Digital Policing in India presents an emerging perspective where data-intensive and networked technologies are leveraged to enhance the capacities of the State in policing, investigating, and managing public order. From facial recognition, predictive policing, surveillance cameras, and cyber surveillance, to closed-circuit television networks, and interlinked data banks such as the Crime and Criminal Tracking Network and Systems (CCTNS) and the Aadhaar system, such technologies offer new opportunities to extend the reach of the State. Predicated upon an assumed commitment to women's safety, digital policing enables the State to intensify its gaze on the body and its control over it, in ways that often transcend legal scrutiny. This paper contends that such systems stand to inflict distinctly gendered costs. By virtue of their design, algorithms and data registries risk misrecognizing women, transgender persons, and minorities; policing practices may well impose social and legal sanctions for immodest conduct, limiting women's mobility, associations, and autonomy. Through an intersectional feminist lens, this paper examines critical gender issues in digital policing, with specific reference to informational privacy after Puttaswamy, discrimination, intrusive surveillance, bodily integrity (with particular reference to gendered data and reproductive rights), and access to justice, particularly in relation to reporting mechanisms and the adjudication of digital evidence. The paper argues that digital policing, as it is currently conceived, privileges the domain of the State over the rights and safety of civilians. It recommends a comprehensive legal framework, which includes gender impact assessments of policing technologies, restricted use of facial recognition, judicial oversight of surveillance practices, enhanced data protection and survivor-centric legal frameworks, and independent oversight mechanisms.

Keywords: *digital policing, gendered surveillance, feminist legal theory, facial recognition technology, right to privacy.*

INTRODUCTION

Over the last 15 years, policing in India has moved from paper registers and manual identification to digitally mediated detection, verification and prediction. Indeed, the Crime and Criminal Tracking Network and Systems (CCTNS), the country's police-station-level backbone of crime records infrastructure, has itself been adapted to run automated facial recognition searches, illustrating how older e-governance projects have been folded into a newer, more intrusive architecture of technological policing. This has been part of a larger movement toward 'smart' governance in India, where biometric identification, networked databases, artificial intelligence and remote sensing are assumed to be the defaults of the modern administrative and security state, with its police apparatus.

For the purposes of this paper, digital policing refers to the set of practices by which law enforcement agencies use digital technologies like biometric identification, pattern analysis, networked criminal databases, and remote automated surveillance to detect, investigate, predict and respond to crime. It refers to something beyond simply the computerisation of police files; it refers to a shift in policing power from that which is reactive and individualised to that which is anticipatory, continuous, and exercised over populations rather than over suspects. Several such technologies now operate or are being built in Indian policing.[1]

The National Automated Facial Recognition System (NAFRS/AFRS), for which the National Crime Records Bureau (NCRB) invited bids in July 2019, using a detailed proposal document describing the project as an effort to modernise the police force and improve criminal information sharing across units, is intended to leverage and cross-match data from the passport database, CCTNS, the Interoperable Criminal Justice System, the Women and Child Development Ministry's Khoya Paya missing persons portal, and the Automated Fingerprint Identification System. In addition to this national project, Delhi Police, in partnership with the Indian Space Research Organisation, has operated the Crime Mapping, Analytics and Predictive System (CMAPS) since 2015, feeding data to handheld devices linked to a central database of criminal records to guide patrolling and identify crime hotspots. Similar technologies to that of CMAPS have been adopted by several other states, such as Punjab,

[1] Daniel Marciniak, 'Data-driven policing: how digital technologies transform the practice and governance of policing' (PhD thesis, University of Essex 2021)

Uttar Pradesh, and Rajasthan, particularly for facial recognition.[2] These operate alongside expanding CCTV networks, cyber surveillance and communication interception capacities and a growing web of interoperable law enforcement databases, collectively functioning as the infrastructure this paper refers to as digital policing. The case for this infrastructure rests heavily on claims of operational benefit. The push for a national facial recognition system followed a 2018 trial in which Delhi Police used the technology to trace roughly 3,000 missing children within four days, an example regularly invoked by advocates to justify further investment. More generally, it is argued that these tools can speed up the identification and analysis of crime patterns in ways manual human methods cannot match, and allow for more efficient allocation of policing resources. Faster identification of missing persons and unidentified bodies, quicker cross-referencing of criminal records across states, and more efficient deployment of personnel are among the benefits that law enforcement and policymakers point to when talking of digital policing.

However, there are risks that have received comparatively little sustained legal attention in India. Independent assessments note that the accuracy of facial recognition in similar projects has been estimated to be around 70 percent, with a real possibility of false positives, a margin of error with potentially serious consequences once the output is fed into arrest, detention, or prosecution.[3] Predictive policing tools are particularly vulnerable to the structural bias problem since persons from marginalised communities are disproportionately reliant on welfare schemes whose data collection feeds into these very databases; the resulting training data is skewed, and the technology can end up entrenching existing human biases under the guise of neutral computation, a pattern reinforced by feedback loops in which over policed, already marginalised localities are flagged high risk and policed more heavily. This has not been matched by accountability, with very little publicly known about the actual functioning of systems such as CMAPS, given broad exemptions under the Right to Information Act enjoyed by law enforcement agencies, and citizens subjected to predictable policing outputs having no way to contest algorithmic inaccuracies. Even licensing has grown quietly. Revised

[2] Siddharth Mahajan and Rouchi Chaudhary, 'Technological Evolution of Indian Policing from Traditional to SMART Technology' (2025) 6(3) International Research Journal of Multidisciplinary Scope 800 <https://www.irjms.com/wp-content/uploads/2025/07/Manuscript_IRJMS_04072_WS.pdf> accessed 25 September 2026

[3] Sukhvinder Singh Dari et al., 'AI-Powered Criminal Identification in India: Evaluating Human Rights Concerns in Automated Identification Systems' (2025) 1(1) SGS-Humanities & Management <https://spast.org/index.php/sgshm/article/view/5302/479> accessed 25 September 2026

tender documents for AFRS introduced a wide search capability in place of the narrower identity verification functions proposed, without any public clarification of its legal basis or limitations. Questions of privacy, discrimination, opacity and lack of redress recur across all these technologies, but are framed, in most policy discussion, as generic rule of law concerns rather than harms that fall unevenly across different groups.[4] This framing hides how digital policing is experienced differently across genders. Technologies introduced in the name of women's safety have often functioned as instruments of monitoring and control.

Madhya Pradesh's Samman initiative, for instance, required women leaving home for work to register with local police, who would then track their movements ostensibly for their protection, but in practice functioning as a control mechanism, with no say for the women involved over how the resulting data would be collected and used. Such schemes are layered onto a law enforcement system in which women reporting crimes face apathy, victim blaming and lack of gender sensitisation, and in which the police is frequently itself a source of sexual and gendered harassment for trans women and sex workers in particular, for whom expanded police visibility is more likely to augment harm than prevent it.[5] A feminist legal perspective is necessary precisely because it takes this interaction seriously. Feminist scholarship on Indian surveillance has already begun to surface continuities between long-standing systems of social control over women and newer digital surveillance technologies, and to ask what the intensification of surveillance in the name of safety, welfare or inclusion actually means for those targeted. To read digital policing through this lens draws attention to how state power over bodies, mobility and sexual autonomy is reconstituted rather than dissolved by claims of technological neutrality, and to how women and sex workers experience protection and surveillance to be functionally continuous rather than opposed.

Despite this, the existing literature on digital policing in India remains largely gender blind. Legal and policy scholarship on facial recognition, predictive policing, and police databases tend to analyse these technologies through the vocabulary of privacy, proportionality and data protection, general treats the citizen as an undifferentiated legal subject. Meanwhile,

[4] Khushboo Rupani, 'Policing Federalism in the Digital Age: Constitutional Design, State Autonomy and Democratic Accountability' in Saurabh Pratap Singh Rathore and Vir Narayan (eds), *Emerging Challenges and Research Frontiers in Digital Transformation* (1st edn, CRC Press 2026) 179

[5] Meetha V Shenoy et al., 'A Holistic Framework for Crime Prevention, Response, and Analysis with Emphasis on Women Safety Using Technology and Societal Participation' (2021) 9 IEEE Access 66188 <https://doi.org/10.1109/ACCESS.2021.3076016> accessed 25 September 2026

feminist critiques of surveillance have developed mostly outside doctrinal legal scholarship in journalism, sociology and internet freedom advocacy and have rarely been connected systematically to the specific legal and institutional architecture of Indian policing and criminal procedure, including the accountability gaps left open by law enforcement exemptions under the Digital Personal Data Protection Act, 2023. This paper seeks to address this gap by bringing feminist legal analysis directly into the doctrinal and institutional design of digital policing in India.

The central argument advanced in this paper is that digital policing in India, despite its genuine investigative benefits, has developed largely without gender differentiated safeguards, and thus created new, unexamined avenues through which patriarchal and majoritarian control over women's and gendered minority bodies, mobility and privacy can be exercised under the language of safety and crime prevention. Addressing this requires not merely technical or procedural fixes to individual technologies, but a feminist legal reassessment of accountability, consent, and redress within the larger framework of police powers and rights protection in India.

CONCEPTUALISING DIGITAL POLICING IN INDIA

Digital policing as used in this paper refers to the increasing practices through which Indian law enforcement agencies employ digital tools like biometric identification, networked databases, algorithmic analytics, and internet-based surveillance to detect, investigate, predict, and respond to crime. Such practices have evolved from the initial computerisation of police records, the networked integration of police stations under CCTNS from 2009, which allows for a single searchable system across stations and the current phase of biometric and predictive convergence, in which data from multiple sources is cross-matched and analysed algorithmically rather than simply stored.[6] This represents a break from the traditional policing, which was largely reactive, station-bound, and dependent on the individual officer's local knowledge and manual record keeping. Technology-enabled policing, in turn, is anticipatory and networked; it aggregates data from jurisdictions, applies pattern recognition to populations in addition to just named suspects, and increasingly substitutes for judgments made on the ground. The remainder of this section will trace that

[6] Mahajan (n 2)

shift technology by technology. The most visible manifestation of digital policing is the proliferation of camera surveillance under the Ministry of Home Affairs Safe City project, funded by the Nirbhaya Fund and launched in 2018 in eight metros. Bengaluru alone saw the addition of over 7,500 cameras, including automated number plate readers, facial recognition units, and drone-based surveillance with a central command and control centre feeding into the National Automated Facial Recognition System (AFRS), which cross-matches with passport, CCTNS, and fingerprint databases to identify suspects and missing persons.[7]

Digital databases and criminal record systems are the visible layer in the growing architecture of records. The CCTNS, under the NCRB, now contains close to 28 crore records linking FIRs, investigations, and charge sheets across over 15,000 police stations. The NCRB also maintains the Central Fingerprint Bureau, the Automated Fingerprint Identification System, and the National Database of Sexual Offenders, and coordinates the Interoperable Criminal Justice System, which links police, courts, prisons, and forensic labs in one data chain. In addition to storage, some agencies are now using this data to predict crime. Delhi Police's Crime Mapping, Analytics and Predictive System (CMAPS), which has been running since 2015 with assistance from ISRO, analyses complaint and crime location data to flag hotspots and to guide patrol deployment. Punjab, Uttar Pradesh, and Rajasthan have all adopted similar tools, particularly around facial recognition-based identification.[8] A further layer focuses on expression online. Dedicated police social media monitoring cells across India's states and union territories grew from 262 in January 2020 to 365 by January 2024, tracking platforms such as Facebook, X, and WhatsApp for content ranging from misinformation to incitement.[9] At a central level, the DRDO developed NETRA, which scans internet traffic for trigger keywords, feeding flagged patterns into wider intelligence systems for cross-referencing against other records.[10]

---

[7] Saumya Baranwal, 'Evolution of AI in Indian Policing and Surveillance: An Analysis' (Proceedings of the International Conference on Socio Legal Intricacies of Artificial Intelligence, Pune, 2026) 131

[8] Abhinav S and Revathi R, 'The Challenges of Crime and Criminal Tracking Networking and System (CCTNS) in Policing' (2025) 2(5) International Journal of Social Science Research 469 <https://www.ijssr.com/papers/volume-2/issue-5/ijssr30658.pdf> accessed 25 September 2026

[9] Amit Kumar and Vibhuti Gupta, 'The Intelligent, Responsible, and Humane Side of Social Media: A Case Study of a Partnership between UP Police India and Facebook Saving Lives' (2024) 39(4) Journal of Police and Criminal Psychology <https://doi.org/10.1007/s11896-024-09667-w> accessed 25 September 2026

[10] Rajan Gupta and Sunil Kumar Muttoo, 'Internet Traffic Surveillance & Network Monitoring in India: Case Study of NETRA' (2016) 8(4) Network Protocols and Algorithms < https://doi.org/10.5296/npa.v8i4.10179> accessed 25 September 2026

All of these systems point to one underlying trend: policing in India is being reorganised around data as its primary raw material. NATGRID, conceived after the 2008 Mumbai attacks and operational since December 2020, embodies this convergence, integrating CCTNS, financial, travel, and telecom records for access by eleven central agencies, with further expansion planned.[11] As databases interconnect and algorithms increasingly mediate decisions made prior by individual officers, questions of who is watched, on what basis, and with what safeguards become harder to answer through traditional, individualised protections.

FEMINIST PERSPECTIVES ON POLICING AND SURVEILLANCE

Feminist legal theory aims to deconstruct the law's alleged neutrality to show how it serves to establish and enforce male dominance over females. According to MacKinnon, the liberal state is not a system that seeks to balance out the conflicting interests of diverse individuals and groups but rather advances male privilege by institutionalising it as law.[12] Therefore, while feminist legal theory does critique explicit discrimination, it goes beyond merely identifying discriminatory statutes by also seeking to deconstruct how discrimination is embedded in seemingly innocuous legal concepts.

The feminist literature has long highlighted police services' patriarchal nature, which manifests in their failure to protect women from domestic violence and the scrutiny that female complainants face when reporting such incidents, with male authorities prioritising their reputation. In context, the policing literature discusses women as victims, the lack of women's representation in the police force, and the tendency of police to harass and abuse women.[13] In India, women are subjected to the same set of prejudiced attitudes, with police forces lacking the gender sensitivity mandated by the new laws on violence against women. Therefore, a feminist view asks the question of how policing tools that aim to make women safer do not fail women by reinforcing their subordination. According to Smart, law is not a

[11] Ryan Shaffer, 'Centralizing India's Intelligence: The National Intelligence Grid's Purpose, Status, and Problems' (2018) 31(1) International Journal of Intelligence and Counterintelligence 159 <https://doi.org/10.1080/08850607.2017.1375336> accessed 25 September 2026

[12] Catharine A MacKinnon, 'Feminism, Marxism, Method, and the State: An Agenda for Theory' (1982) 7(3) Signs: Journal of Women in Culture and Society 515 <http://www.jstor.org/stable/3173853?origin=JSTOR-pdf> accessed 25 September 2026

[13] Cara K Snyder, 'Navigating Online Misogyny: Strategies, Methods, and Debates in Digital Feminism' (2022) 48(3) Feminist Studies 776 <https://www.jstor.org/stable/48760164> accessed 25 September 2026

set of rules that people apply to achieve particular ends; instead, it constitutes social relationships. In particular, she argues that law is constitutive of gender, meaning that it shapes women's status in society. Mackinnon's argument above also implies that law defines the relationship between women and the state, with the state defining women's interests.

Law is, therefore, an instrument of patriarchy that establishes women's dependence on men. When examined through the lens of policing, such a perspective becomes useful in understanding how state surveillance, even when intended to keep women safe, serves to reinforce patriarchy by supervising women, restricting their freedom, and regulating their behaviour. It suggests that the oppression of women is linked to surveillance, which is one way in which patriarchal power relations are manifested.[14] Bartky examines gender relations through the lens of Foucault's ideas on surveillance, arguing that the gender roles assigned to women make female bodies sites of disciplinary power. She suggests that women internalise the idea of being watched and judged for their behaviour, body, and movements accordingly. State surveillance of women builds upon the power dynamics already taking place between men and women, where men monitor women's bodies and judge them.[15] Therefore, the introduction of state-level surveillance does not undermine the patriarchy but rather complements it by introducing another actor in the relationship. Women are subjected to surveillance, both from their families and the state, and consequently, they have to adjust their behaviour based on these expectations.

Therefore, state surveillance of women is inevitably tied up with gender relations, which makes its impact on women's autonomy inherently limited. The feminist literature has questioned the value of privacy as a fundamental right, arguing that the public-private binary is an ideological instrument used to justify the subordination of women. According to MacKinnon, women's domestic roles and responsibilities as wives are framed as private matters that should be decided in the family, despite men and women being unequal in their power within the family unit. The private sphere is, therefore, a site of women's exploitation and oppression, where women are subject to male authority.[16] This perspective has implications for debates on state surveillance of women. As Smart notes above, surveillance

[14] Elizabeth A Stanko, 'The Case of Fearful Women: Gender, Personal Safety and Fear of Crime' (1993) 4(1) Women & Criminal Justice 117 <https://doi.org/10.1300/J012v04n01_06> accessed 25 September 2026
[15] Sandra Lee Bartky, 'Foucault, Femininity, and the Modernization of Patriarchal Power' in Carole R McCann et al. (eds), *Feminist Social Thought* (5th edn, Routledge 2020)
[16] Catharine A MacKinnon, *Feminism Unmodified: Discourses on Life and Law* (Harvard University Press 1988)

of the private sphere is a hallmark of patriarchy, as the private sphere is the realm of domestic, intimate relationships. Women are perceived as their own property, their bodies are considered private, and their autonomy is dependent on their relationship with their husbands or fathers. As such, women are subjected to both familial surveillance of their bodies and state surveillance of their movements and other public behaviours.

While the public sphere has traditionally been a domain of men, it is increasingly regulated by the state, which puts women's autonomy in public in jeopardy.[17] A closely related concern is who benefits from the data collected by surveillance systems. Technology-based policing literature has asked questions about the ethics of surveillance data being used to control and monitor people, particularly vulnerable populations, without their consent. Such a framework, when applied in India, raises difficult questions about how patriarchal the country's police force is, as most of its members are men. Moreover, women are much more likely to be subject to surveillance than to undertake it. Therefore, in relationships where both parties are not equal, such as the police and its wards, the party that has greater control over the other will benefit from surveillance data.

GENDERED RISKS OF DIGITAL POLICING IN INDIA

Gendered Surveillance: Surveillance carried out in the name of women's safety often ends up as an instrument of control over women's own agency rather than protection from outside. Madhya Pradesh's Samman scheme, which required women to register their work location with police to be able to leave home, was a case of women being placed under surveillance without being able to determine the terms of that surveillance, even as it failed to provide any mechanism to control those likely to harm them. The Lucknow Police propose to use facial recognition cameras at twenty identified harassment hotspots to detect changes in women's facial expressions suggestive of discomfort and alert the nearest police station, an initiative that was promptly pointed out by digital rights researchers as instead introducing a permanent state of surveillance as a new normal for women, who would always be on edge that their expression might be scrutinised.[18]

[17] Aditi Narayani, 'Women's Safety in Digital Space' (2024) 70(3) Indian Journal of Public Administration 546 <https://doi.org/10.1177/00195561241271513> accessed 25 September 2026

[18] Dr. Ellina Samantroy, 'Ensuring Social Protection for Women Workers in India: Policy Perspective and Way Forward' in Alakh N Sharma et al. (eds), *Women and Work in India: Challenges, Opportunities and Perspectives for Policy* (Springer Nature Singapore 2026) 507

Facial Recognition and Identification Technologies: The issue of accuracy of such technology, both in general and with regard to gender, has already been raised in the preceding sections. Independent estimates place the accuracy of similar facial recognition technology at around 70 percent, with room for error on either side. Gendered issues arise with regard to emotion or distress recognition technology such as the one proposed by Lucknow Police; if an individual's facial expression is being used as a proxy for their emotional state, there is potential for misunderstanding rooted in cultural differences, as well as a physical disability such as Down syndrome.[19] Trans women and gender non-conforming people have an additional issue with this sort of technology; international studies indicate that facial recognition software performs worse on non-cisgender faces, and a similar issue may affect India's software. In all cases, being incorrectly flagged by such technology as distressed and consequently subjected to police scrutiny carries consequences that such individuals may not be in a position to withstand.[20]

Algorithmic Bias: Policing software that employs predictive analytics is likely to produce systematically biased results if trained on datasets that contain systematic biases, and policing software targeting women is likely to contain systematic biases targeting women. This issue is especially acute in relation to welfare schemes, because the target population for such schemes is usually marginalised women, who are more likely to interact with the state as cardholders rather than taxpayers; any subsequent policing based on this data will necessarily have disproportionately negative consequences on similar demographics. This creates a feedback loop: communities that are policed more closely produce more data, which in turn leads to them being policed more closely in the future.[21] This issue intersects with gender in that poor woman, especially from lower castes or religious minorities, tend to be both more policed and more likely to be falsely identified as such, potentially exacerbating existing social tensions.

---

[19] Meena Rani, 'Impacts and ethics of using Artificial Intelligence (AI) by the Indian Police' (2024) 27(2) Public Administration and Policy 182 <https://doi.org/10.1108/PAP-06-2023-0081> accessed 25 September 2026

[20] Jama Shelton et al., 'Digital Technologies and the Violent Surveillance of Nonbinary Gender' (2021) 5(3) Journal of Gender-Based Violence 517 <https://doi.org/10.1332/239868021X16153783053180> accessed 25 September 2026

[21] Elizabeth E Joh and Thomas Wuil Joo, 'The Harms of Police Surveillance Technology Monopolies' (2022) 99 Denver Law Review Forum <https://digitalcommons.du.edu/cgi/viewcontent.cgi?article=1213&context=dlrforum> accessed 25 September 2026

Digital Profiling: Digital policing often involves constructing digital profiles of individuals based on their online activity, and women are disproportionately affected in ways that cut across all the following issues. The Samman scheme discussed earlier is, in essence, a type of digital profiling of women workers based on their location. The expansion of social media monitoring cells by police across the country, which increased by 365 between 2020 and 2024, represents another form of digital profiling; while such cells serve to identify posts containing misinformation, incitement or other issues, there is no specific consideration for how women's posts might be received or interpreted.[22] Profiling based on locational and digital data is likely to lead to individuals, especially women, being judged or subjected to greater scrutiny based on factors unrelated to any specific crime.

Cyberstalking and Online Harassment: The existing legal framework around technology-facilitated violence against women is narrowly tailored and outdated. Section 354D of the IPC, which was introduced in 2013, criminalises stalking, including visualising any private part of a woman, but only when committed by men against women, not vice versa. The same provision makes exceptions for surveillance conducted by police for the purposes of investigation, which again, implicitly grants police the authority to stalk anyone they suspect to be involved in a crime, without facing consequences for doing so. Courts have shown willingness to interpret Section 354D broadly in appropriate cases, such as in the State of West Bengal v Animesh Boxi, where a man was convicted of stalking and voyeurism and sentenced to five years in prison for hacking into his girlfriend's phone and reading her messages, using both Section 354D and the voyeurism provisions, as well as Section 66 of the IT Act.[23] However, unless and until the courts take up such a case, victims of technology-facilitated violence have to navigate the misogynistic criminal law framework.

Nonconsensual Dissemination of Intimate Material: India does not have an explicit law against nonconsensual dissemination of intimate images or videos. Victims or their families have to rely on Section 66E of the IT Act, which penalises publication of any information about a person without consent; Sections 67 and 67A of the IT Act, which penalise transmitting or publishing material of a sexual nature; and Section 354C of the IPC, which

[22] James P Walsh and Christopher O'Connor, 'Social media and policing: A review of recent research' (2019) 13(1) Sociology Compass <https://doi.org/10.1111/soc4.12648> accessed 25 September 2026

[23] Allison J Brown, 'Non-Consensual Intimate Image Sharing on the Internet: Regulating Betrayal in Jamaica and India' in Hopeton S Dunn et al. (eds), *The Palgrave Handbook of Everyday Digital Life* (Springer International Publishing 2024) 187

penalises voyeurism. Legal scholars critique this framework as ill-suited to the issue at hand, since it was not designed to address nonconsensual dissemination or the rights of women over their bodies, but rather to criminalise obscenity.[24] The actual prevalence of the issue is difficult to estimate, but based on NCRB crime statistics, it is safe to say that it affects thousands of women every year; as of Crime in India 2022, 6896 cases of publishing or transmitting obscene or sexually explicit material were registered with the police nationwide. As mentioned, this figure represents only a small fraction of actual incidents due to social taboos around the issue. The Madras High Court is currently working on a standard operating procedure for dealing with nonconsensual dissemination cases, which would address some aspects of the issue; meanwhile, existing digital policing mechanisms are not equipped to handle such issues due to the speed with which such material circulates online after being posted.[25]

Women at Higher Risk: The issue of policing technology and methods affecting vulnerable women disproportionately intersects with all of the above issues. Commercially available stalker ware such as Spyzie allows abusers to keep tabs on everything a targeted person does on their phone, including messages, calls and location; women who are victims of such surveillance often only cease being monitored when they sever contact with their abuser. Policing technology designed to investigate digital evidence from stalker ware falls under the same category of surveillance as control, with women being subjected to greater scrutiny of their digital lives than most men are likely to experience.

Digital evidence collection techniques are similarly unsuitable for investigating trafficking, where such technologies tend to serve to document the rescue of trafficked persons rather than investigate the trafficking network itself, with women's lives being subjected to greater scrutiny at multiple steps, such as when they are registered for welfare, when their documents are examined, and when their biometrics are taken. Sex worker collectives have long objected to the conflation of sex work and trafficking by law enforcement, arguing that it serves to undermine sex workers' autonomy by removing their ability to choose clients, negotiate payment and working conditions, and hold law enforcement accountable.

[24] Advaith Raj, 'THE OFFENCE OF OBSCENITY UNDER THE INFORMATION TECHNOLOGY ACT, 2000 AND THE INDIAN PENAL CODE' (2020) 19 Supremo Amicus 26 <https://supremoamicus.org/wp-content/uploads/2020/07/A1-5.pdf> accessed 25 September 2026

[25] Chandan Mukherjee et al., 'Crimes against Women in India: Analysis of Official Statistics' (2001) 36(43) Economic and Political Weekly <https://www.jstor.org/stable/4411293> accessed 25 September 2026

Technologies intended to combat trafficking without targeting its financial underpinnings do not differentiate between sex workers who willingly engage in sex work and those who are trafficked, subjecting both to greater scrutiny by the state.[26]

LEGAL AND REGULATORY FRAMEWORK GOVERNING DIGITAL POLICING IN INDIA

Constitutional Framework –

Articles 14 and 15: Equality and the Problem of Algorithmic Bias: Article 14's guarantee of equality before the law, and Article 15's prohibition of discrimination on grounds of sex, are both implicated by automated policing technologies. Facial recognition and predictive policing tools trained on historical arrest data may perpetuate the gendered and communal biases ingrained in such data. However, both Articles 14 and 15 enable legal challenges to a specific discriminatory outcome after the fact; neither provides an ex-ante obligation on the police to audit a facial recognition or analytics tool for disparate impact before release. The guarantee of equality is real, but it is a reactive protection, not the preventive safeguard typically recommended by algorithmic accountability scholarship.

Article 19(1)(a) and (d): Speech, Movement, and the Chilling Effect: Digital surveillance can also involve freedoms of speech and expression and of movement. For women, particularly journalists, activists, and those facing online harassment, the awareness of being watched, tracked, or intercepted (whether by CCTV-linked facial recognition in public places) has a chilling effect on both expression and mobility, which is difficult to litigate precisely because it rarely takes the form of a single, identifiable violation. Article 19's doctrine of identifiable restrictions on identifiable speech is not well suited to capturing this diffuse, anticipatory harm.

Article 21 and the Doctrinal Anchor of Privacy: The starting point for any consideration of digital policing in India is Justice K.S. Puttaswamy (Retd.) v Union of India, where a nine-judge bench of the Supreme Court unanimously held that the right to privacy is a fundamental right, intrinsic to Article 21, and implicitly protected under Articles 14 and 19

[26] Suraj Mandhan et al., 'Engineering the Technological Digital Danger: Rising Threat of Cyber Crimes against Women' (International Conference on Computational Engineering, Sensing Technology and Management, Sydney, 2025) 1 <https://doi.org/10.1109/ICCETM66557.2025.11557906> accessed 25 September 2026

as well. The Right to Privacy as enshrined in Articles 14, 19 and 21 of the Constitution of India is therefore a fundamental right. The Court laid down a stringent proportionality test, holding that any law that intrudes on the privacy of individuals must satisfy the requirements of legality, legitimate state aim, and proportionality between means and ends, to be evaluated through the lens of the just, fair and reasonable test as well. The same verdict also overturned the narrow interpretation of privacy as laid down in M.P. Sharma and Kharak Singh, which permitted indefinite surveillance without any justificatory judicial oversight.[27]

The General Criminal Law Framework –

The Information Technology Act 2000: The IT Act governs state access to electronic communications. Section 69 grants the Central and State Governments the power to direct the interception, monitoring, and decryption of information in the interest of national security, public order, or the prevention of incitement to an offence (under the IT (Procedure for Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009). Section 69A permits the blocking by the state of access to information. Section 69B permits the monitoring of traffic. Each is applied by executive order (not a warrant), with a review by a committee of senior bureaucrats as the sole judicial safeguard. Sections 43 and 66 criminalise unauthorised access to computer systems and computer-related offences, and Section 66C covers identity theft, while Section 66E specifically criminalises the capture or publication of images that violate privacy. Sections 67 and 67A make the publication of obscene and sexually explicit material electronically a crime. Section 79 gives intermediaries a safe harbour from liability for third-party content provided they exercise due diligence, as now elaborated in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

In Shreya Singhal v Union of India, the Supreme Court held that Section 66A was unconstitutionally vague, read Section 79 to require a court or government order before an intermediary could delete objectionable content, and thus that a content platform could not delete content without judicial process in response to a harassment complaint, a landmark

[27] Pratyaksh Joshi and Dr. Yogesh Wamankar, 'ALGORITHMIC POLICING AND DUE PROCESS IN CYBERCRIME INVESTIGATIONS: A CONSTITUTIONAL ANALYSIS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION' (2025) 2(2) ShodhSamajik: Journal of Social Studies 153 <https://doi.org/10.29121/ShodhSamajik.v2.i2.2025.57> accessed 25 September 2026

ruling. In October to November 2025, MeitY notified amendments to the 2021 Rules providing statutory definitions for information that is synthetically generated and a requirement that such information be labelled, permanently tagged, and verified on significant social media intermediaries. The amendments were notified by the Ministry of Electronics and Information Technology under Section 87 of the IT Act, 2000, and commenced on November 15, 2025. This marks the first explicit statutory recognition in Indian law of deepfake-type content, which has acute gendered implications given the prevalence of nonconsensual synthetic sexual imagery targeting women, but it regulates the labelling and takedown by platforms of such content, not its production, and does not create a free-standing offence beyond those already found in Sections 66E, 67 and 67A of the IT Act.[28]

The Bharatiya Nyaya Sanhita 2023: The Bharatiya Nyaya Sanhita 2023 replaces the Indian Penal Code, having been enacted on December 25, 2023 and coming into force on July 1, 2024, for the purposes of digital policing, two provisions are most significant. Section 77 preserves the voyeurism offence, criminalising watching or capturing (and disseminating) images of a woman engaged in a private act without her knowledge. The offence encompasses watching or capturing the image of a woman engaging in a private act in circumstances where she would have an expectation of not being observed, or disseminating such an image, with enhanced punishment on a second conviction. Section 78 criminalises stalking. Stalking includes monitoring a woman's use of the internet, e-mail, or any other electronic communication, and is punishable with up to three years in imprisonment on first conviction and up to five years on a subsequent conviction. This provision, however, embeds the single most striking gendered gap in the entire framework, which deserves to be read closely rather than passed over.

The Bharatiya Nagarik Suraksha Sanhita 2023: The BNSS, which replaces the CrPC, updates criminal procedure to meet the demands of digital investigation. It allows trials, inquiries, and recording of evidence and statements in electronic mode, and also allows police to gather biometric samples, including fingerprints and voice, from those not arrested. The new code also mandates forensic investigation for offences carrying seven years or more of

[28] Debarati Halder, 'Information Technology Act and Cyber Terrorism: A Critical Review' (2011) SSRN <https://doi.org/10.2139/ssrn.1964261> accessed 25 September 2026

imprisonment, allows trials and proceedings to take place in electronic mode, and mandates collection of samples beyond those who have been arrested. Section 176 makes forensic investigation mandatory for offences carrying seven or more years of punishment, indicating a presumption that digital and forensic evidence will play an important role in future prosecution of crimes. However, what the BNSS does not do is create a specific regime for digital search and seizure. Searches and seizures of phones, laptops, and cloud accounts continue to take place under general powers of production of documents and search warrants, interpreted to apply to electronic records as well, but without specific procedures or safeguards, such as standards of forensic imaging, minimisation of irrelevant personal data caught up in a search, or rights of a woman complainant or accused to keep private images and messages out of the wider file. Since investigation into mobile phone records of the accused and complainant, often a woman, forms such a large part of investigations into offences against women, this represents a lacuna in the procedural safeguards that the BNSS provides for digital evidence and data.

The Bharatiya Sakshya Adhiniyam 2023: The BSA replaced the Indian Evidence Act, and amends the admissibility regime for electronic evidence (the successor to the old Section 65B certificate, now Sections 61 to 63) and extends the statutory definition of document and evidence to explicitly include electronic and digital records. This is a welcome change, if only for removing uncertainty about whether WhatsApp chats can be used as evidence (important in prosecutions of cyberstalking, voyeurism and online harassment, where the evidence is, to a great extent, digital).[29]

Cybercrime Provisions and Gendered Digital Offences: Considered collectively, the IT Act and the BNS create a functional, if scattered, cybercrime regime. Section 66C and 66D of the IT Act address online fraud; Section 66E and 77 of the BNS address nonconsensual image capture and voyeurism; IT Act Sections 67/67A/67B address obscene and sexually explicit electronic content and child sexual abuse material; and BNS Section 78 addresses cyberstalking. There is no single, named offence of nonconsensual dissemination of intimate images (revenge pornography) or of AI-generated sexual imagery. Victims and prosecutors

[29] Shreshtha and Renu, 'Digital Obscenity and Criminal Justice: Examining India's Evolving Legal Framework for Pornographic Content in the Digital Age' (2025) 8(5) International Journal of Law Management & Humanities 2172 <https://ijlmh.com/paper/digital-obscenity-and-criminal-justice-examining-indias-evolving-legal-framework-for-pornographic-content-in-the-digital-age/> accessed 25 September 2026

must piece together a case from Section 66E, Sections 67 and 67A, and the voyeurism provision, each of which was drafted with a slightly different fact pattern in mind (unauthorised capture, obscenity, or nonconsensual observation, respectively), rather than the deliberate downstream circulation or synthetic fabrication of an image. The 2025 IT Rules amendment on synthetic media adds a labelling and platform accountability layer but, as noted above, does not create a standalone offence of producing nonconsensual synthetic sexual content, leaving prosecutors to rely on the same older provisions.

The reporting architecture, the National Cyber Crime Reporting Portal, the women and children specific cybercrime reporting wing under the Indian Cyber Crime Coordination Centre (I4C), and state cyber cells, provides an easily accessible first point of contact, but conversion of a complaint into an FIR, and an FIR into a forensically supported prosecution, is contingent on the district-level capacity discussed in connection to the BSA. The gap between an easy-to-file online complaint and a functioning evidentiary pipeline is itself a gendered access to justice concern, since it is disproportionately women who are directed towards these portals for harassment, stalking, and image-based complaints.[30]

RULES, GUIDELINES, AND POLICIES SPECIFICALLY GOVERNING DIGITAL POLICING INFRASTRUCTURE

Automated Facial Recognition and the Absence of Statutory Backing: The NCRB's proposed Automated Facial Recognition System, which would ingest CCTV, passport, CCTNS, and other databases into a singular searchable identification platform, has been challenged since its inception because no statute authorizes its use. The Internet Freedom Foundation's legal notice to the NCRB argued that the project rests on an absence of any statutory or executive legal basis, fails the legality, legitimate aim, and proportionality conditions required under the Puttaswamy judgment, and provides no concrete limitation on how identified individuals' images may be stored or used.[31]

Safe City Projects and the Protective Surveillance Paradox: Nirbhaya Fund-financed Safe City projects, which have expanded CCTV and analytics infrastructure in several major cities

[30] Shruti Bist, *Cyber Crime against Women in India: Investigative and Legislative Challenges* (BlueRose Publishers 2020)
[31] Smriti Parsheera, 'Adoption and Regulation of Facial Recognition Technologies in India: Why and Why Not?' (2019) Data Governance Network Working Paper 05 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3525324> accessed 25 September 2026

in the name of women's safety, illustrate a distinct feminist concern. Surveillance justified as protection can simultaneously increase the state's visual and data footprint over women's ordinary movement through public space, with no independent evaluation of whether increased camera density has in fact reduced the harms.[32] It was funded to address, and no data protection floor governs how footage of women in public is retained, shared, or repurposed for unrelated policing objectives. The same infrastructure built to respond to violence against women can be, and in several documented instances has been, redirected toward general purpose crowd or activity monitoring without any statutory requirement that its use remain confined to its stated protective purpose.

Predictive Policing and Database Interoperability: State-level predictive policing and crime mapping pilots, layered atop CCTNS linked databases, generally operate as internal police department tools rather than public audited systems. There is no statutory disclosure obligation requiring a state police force to publish the variables its predictive model uses, and no external body is empowered to audit such a model for the same gender and community-linked bias concerns that attach to facial recognition.

Police Modernisation and Digitisation Initiatives: The Crime and Criminal Tracking Network and Systems (CCTNS) and the Interoperable Criminal Justice System (ICJS) provide a shared digital record tying together police, courts, prisons, prosecution and forensic laboratories, while the Emergency Response Support System (Dial 112) and the Digital Police Portal offer citizen-facing points of digital access. The Bureau of Police Research and Development lays out advisory standards for state cyber forensic laboratories.[33] These schemes, funded and promoted as efficiency and modernisation measures, share a common feature of relevance: they were conceived and rolled out in executive policy and budgetary allocation, and not through legislation that would set out limits on data sharing between the databases being tied, audit trails of who accessed a given record and why, and a citizen's right to correct erroneous entries that follow her across the interoperable system. Policing infrastructure's digitisation has, in short, comprehensively outpaced the legislative

[32] Shweta M Adur and Shreyasi Jha, '(Re)centering street harassment – an appraisal of safe cities global initiative in Delhi, India' (2018) 27(1) Journal of Gender Studies 114 <https://doi.org/10.1080/09589236.2016.1264296> accessed 25 September 2026

[33] Amit Kumar Singh and Prof. (Dr.) O P Rai, 'Transforming Policing in India: Legal and Institutional Perspectives for Strengthening Criminal Justice Delivery' (2026) 8(1) Ianna Journal of Interdisciplinary Studies 30 <https://unijisedu.com/index.php/ijis/article/view/223> accessed 25 September 2026

architecture that would usually accompany the creation of a linked, searchable, cross-agency database of citizens' criminal and biometric records.

DIGITAL POLICING AND ACCOUNTABILITY IN INDIA

Algorithmic Accountability: In the sense of Bovens (2007), accountability is a matter of a relationship. An actor has to explain and justify his or her conduct to a forum, and this forum can judge this conduct and impose sanctions. Algorithmic accountability is the application of this concept to systems whose outputs inform policing decisions. It means that those who design, procure, deploy and rely on such systems need to be able to explain how they work, allow for independent scrutiny, and provide remedies for the harm they cause.[34] Policing needs this concept because systems are opaque and spread responsibility around, and they repeat the same error for every person that they process. Commercial gender classification tools, for example, reported error rates of up to roughly 35 per cent for darker-skinned women, compared to under 1 percent for lighter-skinned men.[35] A feminist perspective adds the question of who can actually make use of an accountability mechanism. A remedy that requires legal literacy, money and public exposure is not accessible to the women who are most affected.

Who Should Be Accountable? The chain of responsibility extends from the frontline officer up to police leadership, the central and State executive, technology vendors, and the entities that provide data. Present practice tends to single out the most visible and least powerful link, the officer who acted on the output. Instead, responsibility ought to rest where power over design and deployment is actually exercised. Primary responsibility to the affected person should fall on the State and the deploying police authority, given that Indian courts already grant public law compensation for constitutional violations committed by State agents. Officers stay accountable for misuse or bad faith, while vendors are answerable to the State through contract.

Police and Judicial Oversight: The existing mechanisms of police accountability, such as departmental inquiries, Police Complaints Authorities, and Human Rights Commissions,

[34] Mark Bovens et al., 'DOES PUBLIC ACCOUNTABILITY WORK? AN ASSESSMENT TOOL' (2008) 86(1) Public Administration 225 <https://doi.org/10.1111/j.1467-9299.2008.00716.x> accessed 25 September 2026
[35] Morgan Klaus Scheuerman et al., 'How Computers See Gender: An Evaluation of Gender Classification in Commercial Facial Analysis Services' (2019) 3(CSCW) Proceedings of the ACM on Human-Computer Interaction 144 <https://dl.acm.org/doi/pdf/10.1145/3359246> accessed 25 September 2026

none of which were designed for algorithmic conduct, are ineffective for policing that is conducted through algorithms. A woman placed on a watch list or who is the object of a predictive algorithm rarely knows of it, and case records rarely indicate that an automated process triggered a police response. In the direction of CCTV cameras in police stations to deter custodial torture, the Supreme Court has mandated their use to deter custodial abuse.[36] Digital policing turns the gaze of technology back on the citizen and leaves the police organisation unreviewed. Judicial oversight is grounded in a Puttaswamy jurisprudence, which requires legality, a legitimate aim and proportionality for any intrusion on privacy. Its limits are largely theoretical. Interceptions are authorised by the executive, subject to its review, and there is no independent judicial warrant. Judicial review is available only after harm has occurred and only if the person targeted knew she was being targeted. In the litigation over Pegasus, the Supreme Court declined to accept a bare assertion of national security and appointed a technical committee, the findings of which were inconclusive.[37] Courts should treat a match by algorithm as an investigative lead and not as proof, and should require disclosure of error rates and reference databases before relying on them.

Legislative Oversight: Parliament has not authorised facial recognition or predictive policing through statute. Their deployments are based on tenders, executive orders and general police powers, which are not compatible with the legality requirement as interpreted in Puttaswamy. The Digital Personal Data Protection Act, 2023, section 17(2)(a) also grants the Central Government the power to exempt notified State instrumentalities from the entire Act. Therefore, Parliament reserves its right to decide, on a case-by-case basis, which instruments of the State are exempt from the statute.[38] Legislative accountability would require that specific statutes be enacted for each technology, each of which would then need to periodically report to Parliament on their usage, error rates, and complaints, with sunset clauses that require reauthorization.

---

[36] Temitayo Isaac Odeyemi and A Sat Obiyan, 'Digital policing technologies and democratic policing: Will the internet, social media and mobile phone enhance police accountability and police–citizen relations in Nigeria?' (2018) 20(2) International Journal of Police Science & Management 97 <https://doi.org/10.1177/1461355718763448> accessed 25 September 2026

[37] Cressida Renggi Saputra et al., 'The Urgency of Reformulating Digital Policing Regulations within the Framework of E-Polmas and Police 5.0 to Address the Legal Vacuum regarding the Use of Artificial Intelligence in the Field of Public Order and Security' (2025) 3(2) Greenation International Journal of Law and Social Sciences 490 <https://doi.org/10.38035/gijlss.v3i2.488> accessed 25 September 2026

[38] Kanakshi Nema et al. 'AI-Driven Policing and Intelligent Network Governance: Legal Frameworks, Privacy, and Accountability in Smart Public Safety Systems' in Leo SF Lin et al. (eds), *Advances in Smart Heterogeneous Networks for Policing and Crime Prevention* (IGI Global Scientific Publishing 2026) 55

FEMINIST ANALYSIS OF DIGITAL POLICING: KEY FINDINGS

The analysis above of India's legal framework and its accountability gaps leads to a single core conclusion. Digital policing is not neutral with respect to gender, and it is precisely its professed neutrality that allows it to reproduce the very hierarchies it claims to fix. Facial recognition, predictive analytics, CCTV networks, the Crime and Criminal Tracking Network and Systems (CCTNS) and cyber surveillance tools are typically portrayed as objective instruments, yet they rest on historical police data, are built by institutions with a well-documented history of under-recording and dismissing women's complaints, and operate within a social order that already regards women's mobility, sexuality and speech as matters to be controlled. Technology, then, does not stand outside patriarchy; it takes on patriarchy's categories and cements them into code.

Biased data produces biased results, as studies like Buolamwini and Gebru's Gender Shades demonstrated when they found facial analysis systems performing significantly worse on darker-skinned women, and the veneer of mathematical objectivity makes such results harder to challenge than a constable's discretion. This also calls into question the assumption that greater surveillance translates into greater safety for women. Programmes such as Safe City projects and women safety applications are built on a protectionist logic that places risk in public space and responds with watching, even though much gender-based violence is intimate, domestic, online or carried out by known persons, and largely escapes what a camera can detect or deter. Evidence that surveillance genuinely reduces violence is scarce, while evidence that it reshapes who is watched is abundant.

Women may be monitored, tracked and profiled in the name of protecting them, which quietly revives the old paternalistic notion that women's safety is best secured by curtailing their freedom rather than by disciplining those who threaten them. The privacy security debate is frequently presented as a trade-off between an abstract individual right and a collective good, but a feminist reading rejects that framing, since for women privacy is not a luxury set against safety; it is a precondition for it. Bodily autonomy, decisional freedom and informational self-determination, all recognised within Article 21 by Justice K.S. Puttaswamy v Union of India, safeguard a woman's capacity to seek help, leave an abusive home, obtain reproductive care or report an offence without fear of exposure, and a data trail stored in poorly secured police databases can be exploited by abusers, leaked, or used to stigmatise

complainants. The broad state exemptions under the Digital Personal Data Protection Act, 2023, combined with the lack of a dedicated statute regulating facial recognition and predictive policing, mean that the constitutional standards of legality, necessity and proportionality are seldom applied to these tools in practice, leaving the woman who is watched with few means to contest how she is watched. This raises the question of who gains and who carries the risk. The benefits of digital policing, such as administrative efficiency, procurement contracts, political visibility and the symbolic reassurance of doing something, accrue mainly to the state and to private vendors, while the risks of misidentification, over-surveillance, data breaches and secondary misuse fall on those with the least power to demand redress, and since accountability for algorithmic error remains diffused among police, vendors and policymakers, the burden of proof effectively shifts onto the person who is harmed.

Dalit, Adivasi and Muslim women, migrant and informal workers, sex workers, transgender persons, and poor women in over policed neighbourhoods experience digital policing as an extension of existing suspicion, in which a camera or database may serve less as a shield than as a tool of profiling, moral policing and criminalisation, while women with limited digital literacy or access confront a different exclusion as complaints, verification and remedies move to online platforms they cannot easily use. It follows that those technological fixes for gender-based violence cannot succeed on their own terms. They can aid investigation, evidence gathering and faster response, but when embraced as a substitute for structural reform they risk generating new forms of control, turning a problem of power into a problem of data.

A truly feminist approach to digital policing would invert how current practice is oriented, putting women's rights, consent and participation at the design stage, and insisting on gender sensitive impact assessments, independent audits, transparency regarding algorithmic systems, strict limits on data collection and retention, survivor-centred and trauma-informed reporting channels, and enforceable remedies for wrongful surveillance, while regarding technology as a supplement to, never a substitute for, accountable and gender sensitive human institutions. Put briefly, this paper's findings indicate that the real question is not whether digital tools can make women safer, but whether women themselves

are the ones defining safety, and whether those who deploy these tools can be held answerable to the people they claim to protect.

CONCLUSION

This paper has argued that digital technology can genuinely improve policing and investigation in India but that its benefits are inseparable from the social conditions in which it is built and used. Tools such as CCTV networks, facial recognition, predictive analytics, integrated databases and cyber forensic capabilities can speed up the tracing of suspects, strengthen the collection of evidence, improve coordination between agencies and widen the channels by which women can report crime, in principle, and yet the preceding chapters have shown that technological policing is not automatically neutral. These systems rely on historical data, institutional practices and design choices that carry existing social assumptions, and their apparent objectivity makes discriminatory outcomes harder to detect and to challenge.

The feminist analysis developed here has shown that gender and other social inequalities shape how surveillance affects individuals. The same technology may protect one woman while exposing, profiling or controlling another, and caste, religion, class, sexuality, gender identity and digital access determine who is watched, who is believed and who is left without remedy. Increased surveillance cannot be equated with increased safety, especially where violence is intimate, online or committed by persons known to the victim, and where the protective language of women's safety can revive older logics of paternalism and control.

The examination of India's legal framework and of accountability gaps has further shown that constitutional guarantees under Articles 14, 15 and 21 and the protections of the Digital Personal Data Protection Act, 2023 and the new criminal codes do not yet safeguard against wrongful surveillance and misuse of personal data, given the broad exemptions available to the state and the diffusion of responsibility between police, vendors and policymakers, for this reason privacy, dignity, equality and accountability must remain at the centre of any debate on digital policing, not as an obstacle to effective law enforcement but as the conditions that make it legitimate and trustworthy, since women are least likely to report crime to a system they fear will expose or misjudge them. What India needs is a framework that balances legitimate law enforcement objectives with constitutional rights and gender

sensitive safeguards, built on the standards of legality, necessity and proportionality, and supported by statutory authority for the use of surveillance technologies, independent oversight and algorithmic transparency, limits on data collection and retention, sensitivity assessments and survivor-centred remedies for those harmed. Only when digital policing is so constructed can it serve as a genuine instrument of justice and protection and reconcile the promise of technology with the constitutional commitment to equality and human dignity.