



MSB-International Journal of Interdisciplinary Research

Associating Researchers; Nourishing Innovation

Peer Reviewed

Vol. 4, Issue 3, July 2026-October 2026

01-11, MSB-IJIR

Tech Policing and Constitutional Morality: Under the Aegis of New Criminal Laws

¹Ph.D. Scholar

¹Dharmashastra National Law University, Jabalpur

Email: abhinavmphd@mpdnlu.ac.in

ORCID ID: 0009-0006-5254-4749

Abstract

Technology is reshaping the way the State investigates crime, gathers evidence, identifies suspects and carries out criminal investigations. The new criminal laws, namely, Bharatiya Nyaya Sanhita, 2023, Bharatiya Nagarik Suraksha Sanhita, 2023 and Bharatiya Sakshya Adhiniyam, 2023, have enabled the digitally mediated criminal process by adopting electronic communication, audio-video recording, electronic proceedings, and recognition of electronic and digital evidence. These changes can help to be more efficient and to document more, but also have constitutional aspects that need to be addressed: privacy, dignity, autonomy, equality, liberty, and procedural fairness.

This study contrasts the concept of technology mediated policing with constitutional morality and suggests that the power and capacity to do something does not necessarily imply the authority to do it constitutionally. It examines the nature of digital surveillance, facial recognition, biometric identification, algorithmic decision making, predictive policing and digital evidence, focusing on algorithmic bias, opacity, the quality of data, the digital divide, function creep and evidentiary reliability. The paper also goes further in the concept of technological over-criminalisation, how data-driven systems can fuel suspicions and surveillance, by identifying automated alerts, automated profiling, and automated false positives.

The research further aims to have constitutional morality as a prospective principle of institutional design, one that must be respected in the whole technological lifecycle, from legality, necessity, proportionality, equality, transparency, accountability, through to effective remedy. It finds that the three criminal laws are not a blanket constitutional mandate for technologically augmented policing in the sense of making the technology secondary to the constitutional boundaries on the capabilities of the State.

Keywords: Tech policing; constitutional morality; digital evidence; surveillance; facial recognition; biometric data; privacy; proportionality; algorithmic bias; over-criminalization

Introduction

AI and its growing impact on Global Regime is profound with global economy and race for superpower. AI is now being integrated in various systems not limited to technical advancement but a strong want is evident in distinct economic sectors. (Cukier, 2013) Its undisputed that AI has benefited individuals at large and has warranted growth and ease for various sectors. Although such advent has drawn various concerns both ethical and legal. The recent Criminal Law Reform has brought a special focus towards use of Technology in Justice Administration System. This study aims to consider technology-mediated policing in the perspective of constitutional morality. The new Criminal Laws, namely, Bharatiya Nyaya Sanhita, 2023 (hereinafter BNS), Bharatiya Nagarik Suraksha Sanhita, 2023 (hereinafter BNSS), and Bharatiya Sakshya Adhiniyam, 2023 (hereinafter BSA), enhance criminal administration by acknowledging digital evidence and broadening electronic processes, yet their constitutional infirmity hinges on whether technology-driven policing meets the criteria of legality, necessity, proportionality, transparency, non-discrimination, and accountability.

Incubation of technology in BNSS for conducting investigation is appropriately fitting yet lacks potent expertise. Criminal Justice relies on information, although technology has inculcated new scales, speed, and persistence of activities concerning investigation (Redmayne, 2010). Using Digital Surveillance Tools such as AI Cameras and Tracking Systems has brought a drastic shift in how security agencies and justice department impart their function.

Use of AI in Criminal Administration has become more of an actual idea rather than being just a fictional story from the past. In 2002, a movie- *Minority Report*, was released reflecting AI as a tool to predict crime. Backdrop of the story concerned use of AI in tracing delinquents for the possibility of crime that could be committed in near future. Decades later, making an interesting comparison with the movie, the then Chief Justice of India, Dr. D.Y. Chandrachud highlighted that there were significant risks associated with the use of artificial intelligence (AI) to predict crimes (Kumar, 2024). In 2022 a study revealed, algorithms have the ability to predict crime a week in advance (Wood, 2022), and they also reinforce existing biases (Kristian Lum, William Isaac, 2016). Moreover, contending to the more pressing issue, that whether by the use of technology- police and investigating authorities can confine to the moral and legal boundaries of equality, dignity, privacy, autonomy, liberty and procedural fairness.

In particular the article collectively explores the digital divide, algorithmic bias, inadequate or dubious data sets, opacity of automated decision making, over-criminalisation of automated data and function creep. It is clear that it differs from the question of whether a specific surveillance or identification technology is constitutionally valid, and also from the question of whether the code mandates the facilitation of digital criminal procedure (Joseph Shine versus Union of India, 2019).

The underlying premise is that technology itself is not a means to State power. Technology can help police, but it will not expand the constitutional boundaries that must be adhered to for policing.

Information is a long-time cornerstone of criminal justice. Police officers monitor behaviour, make notes, gather physical evidence, determine who is responsible and figure

out what happened. In each of these activities, technology alters the scale, rapidity and duration of these activities. A camera can capture thousands of people in one location; a digital database can store information until after the initial investigation is complete, a digital device can develop a communications and activities history of individuals; and an algorithm can compare massive amounts of information in mere moments of time that would take a human investigator years. (Julie E.Cohen, 2012)

The BNSS explicitly identifies electronic communication and allows for procedures to be carried out by electronic means. For instance, section 105 authorizes the audio and video recording of searches and seizures, so long as it is done via a mobile phone.¹ The information may be provided by electronic communication under Section 173, which requires that a signature be included in the information, as required by the statute.² These provisions enable a criminal process which has more and more come to centre on the digital record.

The BSA will support this change by recognizing electronic and digital evidence as legally admissible evidence. It defines 'document' broadly to include electronic and digital records and sections 61 and 63 detail the conditions for electronic records and their certification and admissibility.³ What is not only being created is more technology in the court room. It can be a redistribution of evidentiary significance: digital traces can come to form a crucial part of the construction of the criminal story.

The creation of a facial image, location record, biometric identifier, device extraction or automated alert is made within an institutional setting. Its reliability relies on the quality of the data, the system design, the threshold value set by the institute, the use operator of the system and the protecting measures on the use of the system. Constitutional morality thus raises a question first: What kind of State power is this that is being built when policing becomes ever more data-driven?

Among the three enactments BNSS is the most directly incorporates technology into procedural practices, it allows for the transmission of information about a cognizable offence by electronic means, subject to the prescribed statutory formalities, and allows for the recording of such information using an audio and video system (preferably a mobile phone) and transmission to the competent judicial or executive authority during a search and seizure operation. Furthermore, Section 530 allows the conduct of trials, inquiry and proceedings to be conducted by electronic means; issues and service of summons and warrants, examination of complainants and witnesses, recording of evidence and appellate proceedings.⁴

These provisions can help to enhance documentation and alleviate reliance on paper systems. Audio-video recording can also provide a record that can be reviewed of a search. Electronic proceedings may overcome geographical obstacles and delays in administrative proceedings. Each of these benefits comes with questions as to implementation, however: who will be in control of the recording, how will it be stored, can it be edited, how long

¹ Bharatiya Nagarik Suraksha Sanhita, 46 of 2023, § 105 (India).

² Bharatiya Nagarik Suraksha Sanhita, 46 of 2023, § 173 (India).

³ Bharatiya Sakshya Adhinyam, 47 of 2023, §§ 61,63 (India).

⁴ Bharatiya Nagarik Suraksha Sanhita, 46 of 2023, § 530 (India).

will it be kept for, who will have access to it, and what will happen if the technology is faulty or a participant cannot access meaningful digital access? (Orin S. Kerr, 2005) (Anuradha Bhasin versus Union of India, 2020).

The BSA provides expressly recognises electronic and digital records within the framework of evidentiary law. Electronic and digital records are part of the concept of a document in Section 2 and are illustrated by electronic messages, server logs, computer or smart phone records, websites, locational evidence and voicemail. An electronic or digital record shall be admissible, subject to the statutory conditions, because it is an electronic or digital record. This section outlines conditions on admissibility of electronic records and the certificate to be provided in the appropriate circumstances.⁵

The implications of the constitution are significant. The evidentiary system relies more and more on the records produced by devices and platforms which may be hard for the accused to understand and/or question as to their operation. However, procedural fairness requires more than a formal admission, so it is not the only requirement. It must provide an opportunity to question authenticity, integrity, provenance, and context and to wonder about the reliability of the underlying data (Eoghan Casey, 2011).

The BNS does not adopt a comprehensive approach to a statutory code on technological surveillance, but simply reorganises and restates criminal offences. It is not, therefore, to be said to be creating a facial-recognition regime in general. It is important for tech policing, because when conduct is considered criminal, the investigation and prosecution of the conduct can be made using procedures and structures of evidence that are digitally enabled as recognised by the BNSS and BSA.

The underlying notion here is towards a restrictive authority to further the use of technology in police driven state, nuances concerning a constitutional power can be exercised to establish balance and harmony among the laws and the rights. Researcher aims to push for Constitutional Morality to be considered here as a law about the use of public power. The issue isn't if police tech is modern, it is towards the constitutionality of the individuals rights. Primarily, the case since technological systems can render coercive practices impartial. A database record can be neutral, an algorithmic score can be scientific and a biometric match can be definitive. In the absence of any constitutional morality, the State can no longer be held accountable for the human impact of such products.

The Vitality of Constitutional Morality is evidently drawn through several landmark cases concerning fundamental rights. In the case of K.S. Puttaswamy, the Court declared privacy a fundamental right, and correlated privacy with dignity, autonomy and protection of individual choice (K.S. Puttaswamy versus Union of India, 2017), the Court declared privacy a fundamental right, and correlated privacy with dignity, autonomy and protection of individual choice. In later constitutional cases the proportionality framework stipulates that interference with fundamental rights must be lawful, serve a legitimate purpose and be necessary and proportionate to the goals pursued and be underpinned by safeguards in the form of a procedure to prevent abuse (Modern Dental College & Research Centre versus State of Madhya Pradesh, 2016).

⁵ Bharatiya Sakshya Adhiniyam, 47 of 2023, § 2 (India).

The constitutional principles expressed by the Supreme Court of India in Maneka Gandhi judgment and then re-stated in Anuradha Bhasin ruling, demands that the use of State power be kept within bounds of fairness, reasonableness, and proportionality. The rules are applied to technologically-mediated criminal investigations, to distinguish between the technical ability of police to gather or process information and the constitutional validity of their action. The use of investigative technologies, therefore, should be based on legal authorization, should have a legitimate purpose, should be proportionate to the legitimate purpose, and should be accompanied by appropriate safeguards that are commensurate to the degree of intrusion in the rights of individuals. (Maneka Gandhi versus Union of India and Ors., 1978) (Anuradha Bhasin versus Union of India, 2020).

Equality and ‘Digital Divide’

The digital divide goes beyond just access to the internet, and includes a range of issues, including access to a smartphone, network quality, digital literacy, access to language-appropriate services, and access to, maintenance of, interpretation of, and challenge of, electronically generated records. Within the criminal justice system, these inequities may result in unequal opportunities for engagement, such as the assumption that some people possess digital skills that are essential for engaging in some aspects of the system. A person accused of an offense or a complainant who cannot access the electronic procedures, electronic notices and/or relevant electronic material could be at a disadvantage compared to a technologically equipped person. Technological modernisation should help, not hinder, access to justice, consistent with the constitutional principles of equality, fairness and reasonableness as stated in Maneka Gandhi and the protection against disproportionate restrictions in Anuradha Bhasin. The principle of the constitution is not that everyone gets equal tech treatment. What the State should not do is to create processes that would mean that being technologically disadvantaged would result in a legal disadvantage (Cohen, 2019). Non-digital alternatives are therefore not failures of technology but equality safeguards. Assisted access, language sensitive procedures are therefore not failures of technology but equality safeguards.

Algorithmic bias

Algorithmic systems are frequently offered as a means of diminishing the subjectivity of humans. However, there are no algorithms that exist outside of social structures. They are based on the training data, selection criteria, variables, labels, thresholds and institutional assumptions. If policing data is historically available showing unequal policing, a predictive and/or classificatory policing system can exacerbate and/or perpetuate that inequity in policing and give the appearance of a technical policing solution (Isaac, Kristian Lum & William, 2016) (Selbst, Solon Barocas, Andrew D., 2016).

Human discretion replaces police discretion as an example of the traditional police discretion. Decision-making regarding the use of algorithms is more diffuse because it is shared among officers, vendors, datasets and software. An afflicted person might not be aware of the reason behind the afflictions.

Constitutional morality is thus, dependent on explainability in relation to the consequence of the decision. If technology is the basis for a consequential police action, the person involved should be able to have access to the material basis of the action, as per legitimate police investigative restrictions, and challenge significant errors.

Digital policing poses a new type of problem to the traditional physical evidence, one that information can survive and be reused. Data collected for Identification is likely to be added to a larger data base. The information that may be gleaned from a location record from one investigation can be unrelated to another investigation and could provide information about a person's associations, movements or private life. The concern with the constitution is not just at collection time, it also applies to retention, access, sharing and re-use.

There is a major exception to the criminal-justice aspect of the Act, namely, section 17(1)(c) of the Digital Personal Data Protection Act, 2023 which excludes certain provisions from its application in cases where the personal data is being processed for the purposes of the prevention, detection, investigation or prosecution of an offence or contravention of law. Safeguards in the criminal justice sector are important due to the statutory role of this sector. In places where the formal duties for data protection don't apply, criminal-investigation databases need to be subject to discussions about purpose, access, retention, correction, deletion, sharing and independent oversight.⁶

A particular function creep is important in limiting a database that is originally intended for a specific purpose may get increasingly used for other purposes. Constitutional response to the question must be purposively limited to the autonomy of the state in its use of data collected for confined means. It should be considered unlawful use by lawful authorities (Helen Nissenbaum, 2010).

There is also an Article 14 concern in the context of algorithmic decision making when there are historical patterns of discriminatory policing which are reproduced and/or amplified by seemingly neutral technological systems. Constitutional equality demands analysis of both the design of the algorithm, as well as the data it's trained on, variables it utilizes, and distribution of its outcomes (E.P. Royappa versus State of Tamil Nadu, 1974) (Anuj Garg & Ors versus Hotel Association of India & Ors, 2008).

Digital Chain of Custody & Due Process

With the shift to electronic evidence comes the opportunity for greater integrity and also new questions arise. A digital record can be replicated exactly but can also be processed and edited, selectively extracted from the record, metadata stripped from the record or presented outside its original context. The statutory obligations of the BSA on electronic records and certification, therefore, are crucial but this does not mean that the legal admissibility is the same as the substantive reliability. For automated tools, some information about the tool and its limitations should be provided where necessary for a fair challenge based on the evidence analysed by the automated tool. (Casey, 2011) (Tech., 2006) (Maneka Gandhi versus Union of India and Ors., 1978) (Selvi & Ors. versus State of Karnataka & Anr., 2010)

Facial recognition technology is a case study that is relevant to the constitutional challenges of technological support of criminal investigation. Facial matching can aid in identification of a suspect during a normal investigation, but does not provide conclusive evidence of identity.

⁶ Digital Personal Data Protection Act, No. 22 of 2023, § 17(1)(c) (India).

They must be judged on the basis of the reliability of the technology and the possibility of error as well as the availability of independent corroborative evidence (Clare Garvie, Alvaro Bedoya, Jonathan Frankle, 2016). There may be variations in accuracy due to the quality of the images, the population conditions, the design of the system and the operational parameters (Joy Buolamwini, Timnit Gebru, 2018). When there is a false match, a series of suspicions can begin that will be hard for the person to clear up. (Intifada P. Basheer, 2025)

The discomfort in the constitution is heightened when it is linked with huge databases and round the clock surveillance. Identification can turn into tracking, tracking can turn into profiling, and profiling can have an impact on the future of police attention. This is why it is important to look at the entire data lifecycle when doing constitutional review, and not just collection. (Helen Nissenbaum, 2010)

The legislation should not grant facial recognition technology a de facto blanket legality nor ban its usage outright. Its constitutional validity should be judged instead based on the presence of clear statutory authorization, on the attainment of a legitimate objective of the State and on the observance of the constitutional necessity and proportionality requirements. Its use should in addition be limited by legally binding provisions on accuracy, human verification, data storage, independent review and effective ways of challenging adverse decisions and rectifying any inaccuracies. The obligations of disclosure and notification also need to be appropriately regulated by suitable procedural protections, taking into account the needs of the continuing investigation, and the rights of those concerned. The constitutional validity of the use of facial recognition must therefore not only rely on its technical potential, it must also be based on the legality, proportionality and procedural accountability of its use (Clare Garvie, Alvaro Bedoya, Jonathan Frankle, 2016)

Too many offences or over-generalisations in the criminal law are usually the focus of over-criminalisation (Sara Sun Beale, 2005) (Stephen F. Smith, 2013). An automated over-criminalisation is another possibility that technology brings. The phrase here does not have the meaning of saying that automated systems have already taken the place of legal judgment but rather it is a description of risk (Victor Rotaru, Yi Huang, Timmy Li, James Evans & Ishanu Chattopadhyay, 2022) (Isaac, Kristian Lum & William, 2016)

The danger is that when data-driven systems increase the number of people, actions or patterns that are the subject of suspicion. With a low threshold for alerts, many false positives can result. After entering an institutional record, an alert could potentially impact any further decisions made, even if it turns out to be incorrect. This can create a vicious cycle, generating more and more surveillance data and more and more suspicion and more surveillance, and so on.

A constitutional morality approach disrupts this circle by questioning whether or not the State is addressing a recognisable harm and whether the State's technological intervention is really needed. Abuse of public resources is a hallmark of the carceral culture of data. The carceral culture of data is characterized by the abuse of public resources (John Stuart Mill, 1921) (Arthur Ripstein, 2006).

The notion of carceral culture can help to uncover why surveillance should be the subject of attention beyond the realm of punishment. The psychological and social context of public life can shift when people are aware their actions, conversations, and/or identities can be tracked at all times. Surveillance can have an influence on behaviour even if there is no prosecution (Neil M. Richards, 2013).

The judiciary has a crucial constitutional role to play in the development of technology in criminal proceedings which respects the fundamental rights and freedoms of individuals. This judicial review should not be limited to the adjudicatory process or only be brought forward on prosecution or when penalties are imposed. In contrast, constitutional review should, when legally possible, be applied to the lawfulness of the investigative procedures, to the proportionality of surveillance, to the compliance with the procedural safeguards and to the authenticity, reliability and admissibility of technologically obtained evidence.

The Supreme Court's jurisprudence on the concept of privacy is important. Puttaswamy considers privacy as a basic right which is connected with dignity and autonomy. In the case of PUCL v. Union of India, it is seen how the procedural safeguards relating to telephone interception came into play (People's Union for Civil Liberties versus Union of India, 1997). Selvi versus State of Karnataka is a landmark case that highlighted the fundamental right of mental privacy and the extent of compelled disclosure of testimonial information under the Constitution (Selvi & Ors. versus State of Karnataka & Anr., 2010). The law of "proportionality" and later the presence of Maneka Gandhi reaffirms the idea that the procedure which impacts on liberty should meet constitutional requirements, not just the mere requirements of the statute book.

Several Constitutional questions push constitutional review beyond the narrow test of any one police incident into an accountability system based on structural issues. The concept of constitutional morality goes beyond the act of invalidating (Nakul Nayak, 2023) (Bagchi, Kanad, 2018). Constitutional morality should not be used merely as a law school jargon to invalidate laws that are unconstitutional. It can be used as a rule of institutional design, in the prospective future. Police Departments, Legislatures, Courts, Prosecutors and Forensic Institutions and Technology Vendors can have a constitutional values perspective in the design phase. (Andre Béteille, 2008)

This can be especially crucial in the case of technology, as technology systems are generally hard to break up when they become institutionalised. Dependencies are created through procurement, historical records are stored in databases, staff is trained on specific platforms and by encouraging interoperability, there is an incentive to share more data. Thus, the use of constitutional morality is more useful in the pre-deployment phase than at the post-deployment phase (Navtej Singh Johar versus Union of India, 2018).

Findings

The Major Laws explicitly encourage a more digitally mediated criminal process, and operate in this larger framework of the criminal process and the evidence. They should not be interpreted to constitute a blanket also of legal authority and constitutional justification for the use of facial recognition or mass surveillance. Existing laws of specialisation and constitutional reasoning are still valid alongside the new criminal laws.

Documentation, accessibility and efficiency can be enhanced by digitalisation provided it is implemented, kept correct and is accessible. Algorithmic systems can perpetuate inequities if trained or tested with incomplete or biased data and can exacerbate inequities

if designed to address it. Digital divide can turn technological disadvantage to procedural disadvantage without assistance, unless kept with other means of getting things done. Since the formal admissibility of electronic evidence doesn't absolve of questions of authenticity, provenance and context, they must have strong integrity and chain-of-custody practices. Constitutional morality can be a prospective governance principle; based on the principles of legality, proportionality, equality, accountability and remedy (Latika Vashist, 2013).

Conclusion

India's march towards technology-aided policing is not an easy case of "modernization" nor is it an easy case of surveillance. It's a change in the way state power engages the individual, a constitutional change. The BNS, BNSS and BSA are the legal framework for a criminal procedure that increasingly plays an important role in electronic communications, audio video procedure and digital evidence. The Criminal Procedure (Identification) Act, 2022 is an additional identification infrastructure. In combination with current policing technologies, these shifts open up new avenues for investigation and avenues for mistakes, exclusion and overreach.⁷

The central constitutional inquiry is not whether technological advancements enable the state to exercise greater surveillance, but whether the exercise of such power is legally authorised, strictly necessary, and proportionate to a legitimate State objective. It further requires scrutiny of whether the information collected remains subjective to effective challenge and whether individuals are afforded adequate legal protection against errors arising from technological systems. The enhanced capacity of the State to monitor, identify, and process information cannot, by itself justify an expansion of its constitutionally permissible power. The foundational premise of the constitutional democracy is that the individual remains protected by the Constitution against arbitrary State action, rather than rendered perpetually exposed to the expanding surveillance capabilities of the State.

⁷ Criminal Procedure (Identification) Act, No. 11 of 2022, §§ 2–4 (India).

References

- Cukier, V. M.-S. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
- Redmayne, A. A. (2010). *The Criminal Process*. 4th ed. Oxford Univ. Press .
- Kumar, A. (2024, April). *Chief Justice of India cites Tom Cruise-starrer 'Minority Report' to make an important point*. Retrieved from <https://www.cnbtv18.com/technology/cbi-raising-day-chief-justice-chandrachud-caution-artificial-intelligence-hollywood-film-minority-report-19390652.htm>
- Wood, M. (2022, June). *Algorithm predicts crime a week in advance, but reveals bias in police response*. Retrieved from Biological Sciences: <https://biologicalsciences.uchicago.edu/news/algorithm-predicts-crime-police-bias>
- Kristian Lum, William Isaac. (2016, October). To Predict and Serve? *Significance* , 13(5), 14-19.
- Joseph Shine versus Union of India, (Writ Petition (Criminal) No. 194 of 2017) (Supreme Court of India 2019).
- Julie E.Cohen. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. Yale University Press.
- Orin S. Kerr. (2005). Searches and Seizures in a Digital World. *Harvard Law Review*, 534–35.
- Anuradha Bhasin versus Union of India, Writ Petition (Civil) No. 1031 of 2019 (Supreme Court of India 2020).
- Eoghan Casey. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press.
- K.S. Puttaswamy versus Union of India, Writ Petition (Civil) No 494 of 2012 (Supreme Court of India 2017).
- Modern Dental College & Research Centre versus State of Madhya Pradesh, Civil Appeal No. 4060 of 2009 (Supreme Court of India 2016).
- Maneka Gandhi versus Union of India and Ors., Writ Petition No. 231 of 1977 (Supreme Court of India 1978).
- Cohen, J. E. (2019). Between Truth and Power: The Legal Constructions of Informational Capitalism. *Oxford Univ. Press*.
- Isaac, Kristian Lum & William. (2016). To Predict and Serve? *Significance*, 14, 14–19.
- Selbst, Solon Barocas, Andrew D. (2016). Big Data's Disparate Impact. *California Law Review* , 104, 671–732.
- Helen Nissenbaum. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- E.P. Royappa versus State of Tamil Nadu, W.P.(CRL.)NO.194/2017 (1974).
- Anuj Garg & Ors versus Hotel Association of India & Ors, (2008)3 SCC 1 (Supreme Court of India 2008).
- Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3d ed. Academic Press .
- Tech., N. I. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publication* , 800-86.
- Selvi & Ors. versus State of Karnataka & Anr., (Criminal Appeal No. 1267 of 2004) (Supreme Court of India 2010).

- Clare Garvie, Alvaro Bedoya, Jonathan Frankle. (2016, October 18). *The Perpetual Lineup: Unregulated Police Face Recognition in America*. Retrieved from Georgetown: Law Center of Privacy and Technology:
<https://www.perpetuallineup.org/>
- Joy Buolamwini, Timnit Gebru. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, 81, 77–91.
- Intifada P. Basheer. (2025). Bias in the Algorithm: Issues Raised Due to Use of Facial Recognition in India. *Journal of Development Policy and Practice*, 61-79. Retrieved from 10 Indian J. Hum. Rts. & Social Just. 1:
<https://doi.org/10.1177/24551333241283992>
- Sara Sun Beale. (2005). The Many Faces of Overcriminalization: From Morals and Mattress Tags to Overfederalization. *American University Law Review*, 747–802.
- Stephen F. Smith. (2013). Overcoming Overcriminalization. *The Journal of Criminal Law and Criminology*, 537–77.
- Victor Rotaru, Yi Huang, Timmy Li, James Evans & Ishanu Chattopadhyay . (2022). Event-Level Prediction of Urban Crime Reveals a Signature of Enforcement Bias in US Cities. *Nature Human Behaviour*, 1056–68.
- John Stuart Mill. (1921). *On Liberty*. Atlantic Monthly Press.
- Arthur Ripstein. (2006). Beyond the Harm Principle. *Philosophy and Public Affairs* , 215, 215–45.
- Neil M. Richards. (2013). The Dangers of Surveillance. *Harvard Law Review*, 1934–38.
- People's Union for Civil Liberties versus Union of India, AIR1997SC568 (Supreme Court of India 1997).
- Nakul Nayak. (2023). Constitutional Morality: An Indian Framework. *The American Journal of Comparative Law*, 354–87.
- Bagchi, Kanad. (2018). Transformative Constitutionalism, Constitutional Morality and Equality: The Indian Supreme Court on Section 377. *Law and Politics in Africa, Asia and Latin America*, 367-80.
- Andre Béteille. (2008). Constitutional Morality. *Economic and Political Weekly*, 35–42.
- Navtej Singh Johar versus Union of India, Writ Petition (Criminal) No. 76 of 2016 (Supreme Court of India 2018).
- Latika Vashist. (2013). Re-thinking Criminalisable Harm in India: Constitutional Morality as a Restraint on Criminalisation. *Journal of the Indian Law Institute*, , 73–93.