Original Article
ISSN (Online): 3049-2319

ShodhSamajik: Journal of Social Studies
July-December 2025 2(2), 153–167

ALGORITHMIC POLICING AND DUE PROCESS IN CYBERCRIME INVESTIGATIONS: A CONSTITUTIONAL ANALYSIS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION

Pratyaksh Joshi [1], Dr. Yogesh Wamankar [2]

[1] Research Scholar, Mansarovar Global University, Sehore, Madhya Pradesh, India
[2] Assistant Professor, Mansarovar Global University, Sehore, Madhya Pradesh, India

Received 28 October 2025
Accepted 29 November 2025
Published 19 December 2025

DOI
10.29121/ShodhSamajik.v2.i2.2025.57

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The increasing reliance on artificial intelligence in cybercrime investigation has significantly altered the manner in which policing power is exercised in India. Law enforcement agencies now employ algorithmic tools for surveillance, pattern detection, suspect identification, and predictive assessment of digital behaviour. While these technologies promise efficiency and enhanced investigative capacity, they simultaneously raise serious constitutional concerns. This paper critically examines whether AI-driven cybercrime investigations are compatible with the guarantees of equality, freedom, and personal liberty enshrined under Articles 14, 19, and 21 of the Constitution of India. It argues that algorithmic policing challenges foundational principles of due process by introducing opaque decision-making, automated suspicion, and data-driven profiling that risk diluting the traditional requirement of reason to believe in criminal investigations. Through a doctrinal analysis of constitutional jurisprudence, statutory provisions governing surveillance and digital evidence, and emerging scholarly discourse on algorithmic governance, the paper contends that the current deployment of AI in cyber policing operates in a constitutional grey zone. The study concludes that without explicit legislative regulation, enforceable standards of transparency and explainability, and meaningful human and judicial oversight, algorithmic policing may undermine procedural fairness and constitutional accountability rather than strengthen the rule of law in India.

Keywords: Algorithmic Policing, Cybercrime Investigation, Due Process, Constitutional Law

1. INTRODUCTION

The rapid digitisation of governance, commerce, and social interaction in India has fundamentally transformed the nature of crime and criminal investigation. Cybercrime has expanded beyond isolated instances of hacking or online fraud to include complex offences such as large-scale financial fraud, identity theft, cyberstalking, ransomware attacks, and coordinated digital conspiracies operating across territorial boundaries Kshetri (2021), MeitY (2023). Traditional policing mechanisms, which rely heavily on physical evidence and territorial jurisdiction, have struggled to respond effectively to crimes that are instantaneous, anonymous, and data-driven in nature Wall (2018).

In response to this growing challenge, Indian law enforcement agencies have increasingly adopted artificial intelligence-based tools to assist cybercrime investigation. These tools include algorithmic data analytics, predictive modelling, facial recognition systems, and automated surveillance technologies designed to process vast volumes of digital information and identify suspicious patterns NITI (2022). The adoption of such technologies is often justified on grounds of efficiency, prevention, and national security, particularly in the context of resource constraints and rising cybercrime caseloads Agarwal and Choudhary (2020).

However, the incorporation of artificial intelligence into criminal investigations represents a significant shift in the exercise of state power. Indian criminal jurisprudence has historically required that investigative action be based on human judgment constrained by legal standards such as reason to believe, proportionality, and procedural fairness Ratanlal and Dhirajlal (2022). Algorithmic policing alters this framework by introducing machine-generated suspicion and probabilistic risk assessments, which may influence or determine investigative decisions without transparent reasoning or meaningful human deliberation Barocas and Selbst (2016).

This shift raises serious constitutional concerns. When algorithmic systems determine who is subjected to surveillance, investigation, or arrest, questions arise regarding equality before law under Article 14, freedoms guaranteed under Article 19, and the right to life and personal liberty under Article 21 of the Constitution of India Puttaswamy v. Union of India, (2017). The Supreme Court has consistently held that any state action affecting personal liberty must follow a procedure that is just, fair, and reasonable, and must not be arbitrary or disproportionate Maneka (1978).

Algorithmic policing also poses challenges to informational privacy and decisional autonomy. The recognition of privacy as a fundamental right under Article 21 has extended constitutional protection to personal data and digital footprints, thereby subjecting state surveillance practices to heightened scrutiny Puttaswamy v. Union of India, (2017). AI-driven cyber policing tools, which rely on continuous data collection, profiling, and automated inference, directly implicate these privacy concerns and demand robust legal justification.

Despite the increasing use of artificial intelligence in cybercrime investigation, India lacks a comprehensive statutory framework regulating algorithmic policing. Existing legal provisions under the Information (2000) and the Code of Criminal Procedure were enacted in a pre-algorithmic era and do not adequately address issues such as algorithmic opacity, bias, explainability, and accountability Bhatia (2021). Even recent data protection legislation provides broad exemptions to the state, thereby limiting its effectiveness as a safeguard against intrusive surveillance practices Srikrishna (2023).

Against this backdrop, this paper examines whether AI-driven cybercrime investigations can withstand constitutional scrutiny under Articles 14, 19, and 21 of the Constitution of India. By adopting a doctrinal and conceptual approach, the study seeks to assess whether algorithmic policing strengthens the rule of law by enhancing investigative capacity or undermines constitutional due process by diluting procedural safeguards and accountability mechanisms.

2. CONCEPTUAL FRAMEWORK: ALGORITHMIC POLICING AND DUE PROCESS

Algorithmic policing refers to the use of automated or semi-automated computational systems to assist law enforcement in identifying, predicting, or responding to criminal activity. In the context of cybercrime investigation, such systems rely on artificial intelligence techniques including machine learning, data mining, and predictive analytics to process vast quantities of digital information and generate outputs that inform investigative decisions Kitchin (2014), Barocas and Selbst (2016). These outputs may include risk scores, anomaly flags, network linkages, or probabilistic assessments of suspicious behaviour. While these tools are often framed as decision-support mechanisms, in practice they can exert significant influence over how suspicion is formed and acted upon by investigating agencies Lum and Isaac (2016).

Due process, as understood within Indian constitutional jurisprudence, is not confined to formal legality but encompasses substantive fairness, reasonableness, and non-arbitrariness in the exercise of state power. Following the decision in Maneka (1978), Article 21 has been interpreted to require that any procedure which deprives a person of life or personal liberty must be just, fair, and reasonable, and not arbitrary, fanciful, or oppressive. This expanded understanding of due process is closely linked with Article 14's prohibition of arbitrariness and Article 19's protection of fundamental freedoms. Together, these provisions impose a constitutional obligation on the state to ensure transparency, accountability, and proportionality in criminal investigations Seervai (2015).

A central concept in Indian criminal procedure is the requirement of "reason to believe." Investigative powers such as search, seizure, interception, and arrest are conditioned upon the formation of an objective belief by the investigating officer, based on relevant material and subject to judicial scrutiny Ratanlal and Dhirajlal. (2022). This requirement serves as a safeguard against arbitrary state action by ensuring that coercive powers are exercised through human judgment informed by legal standards. Algorithmic policing challenges this safeguard by shifting the basis of suspicion from articulated reasons to statistical correlations generated by opaque systems Pasquale (2015).

The opacity of algorithmic systems presents a further conceptual challenge. Many AI tools operate as black boxes, producing outputs without providing intelligible explanations of how particular conclusions were reached. Scholars have noted that such opacity undermines the ability of affected individuals to understand, contest, or challenge decisions that adversely impact them Wachter et al. (2017). In the criminal justice context, this lack of explainability directly conflicts with principles of natural justice and procedural fairness, which require that decisions affecting rights and liberties be reasoned and reviewable.

Another important concept is algorithmic bias. AI systems are trained on historical data that often reflect existing patterns of policing, social inequality, and enforcement priorities. As a result, algorithmic tools may reproduce or amplify discriminatory outcomes, even in the absence of explicit intent Barocas and Selbst (2016). In the Indian context, where socio-economic status, geography, and access to digital infrastructure are deeply uneven, the risk of biased outcomes in cyber policing raises serious concerns under Article 14's guarantee of equality before law Bhatia (2021).

The framework of algorithmic governance also highlights the phenomenon of automation bias, wherein human decision-makers tend to defer to machine-generated outputs, perceiving them as objective or superior to human judgment Citron (2008). In policing, this can result in investigative officers treating algorithmic assessments as determinative rather than advisory, thereby reducing meaningful human oversight. Such deference risks converting assistance into delegation, a shift that is constitutionally significant when decisions affect personal liberty.

Finally, the recognition of informational privacy as a component of Article 21 has added a new dimension to due process analysis in the digital age. The Supreme Court in Justice (2017) held that state action involving the collection, processing, and use of personal data must satisfy the tests of legality, legitimate aim, necessity, and proportionality. AI-driven cybercrime investigations, which depend on continuous data collection and profiling, must therefore be assessed against this constitutional standard. The absence of clear legal authorisation and procedural safeguards in algorithmic policing raises serious questions about its compatibility with the constitutional conception of due process.

This conceptual framework underscores that the constitutional challenge posed by algorithmic policing is not merely technological but normative. It concerns the redistribution of decision-making power between humans and machines and the extent to which constitutional safeguards can survive in an investigative environment shaped by automation, opacity, and data-driven inference.

3. CONSTITUTIONAL FRAMEWORK GOVERNING ALGORITHMIC POLICING IN INDIA

The constitutional validity of algorithmic policing in cybercrime investigations must be examined within the framework of fundamental rights guaranteed under Part III of the Constitution of India. Articles 14, 19, and 21 collectively impose substantive and procedural limitations on the manner in which the state may exercise coercive power, particularly in the domain of criminal justice. The Supreme Court has consistently held that these provisions are not isolated guarantees but form an integrated framework aimed at preventing arbitrariness, protecting individual liberty, and ensuring fairness in state action Maneka (1978), Seervai (2015).

3.1. ARTICLE 14 AND THE PROHIBITION OF ARBITRARY STATE ACTION

Article 14 guarantees equality before the law and equal protection of the laws. Judicial interpretation has expanded this guarantee beyond formal equality to include a prohibition against arbitrary state action. The Supreme Court has held that arbitrariness is antithetical to equality and that any state action which is arbitrary is liable to be struck down under Article 14 E (1974).

Algorithmic policing raises significant concerns under this doctrine. AI systems used in cybercrime investigations rely on data-driven models that classify individuals based on patterns, correlations, and risk indicators. These classifications often operate without transparency and may not be subject to meaningful justification or review Barocas and Selbst (2016). When individuals are subjected to surveillance or investigation based on algorithmic outputs that cannot be explained or contested, the requirement of non-arbitrariness is undermined.

Furthermore, algorithmic systems trained on historical crime data risk reproducing existing enforcement biases. Disparate impact, even in the absence of discriminatory intent, may result in differential treatment of individuals or groups based on socio-economic status, geography, or patterns of digital access Bhatia (2021). Such outcomes challenge the constitutional mandate of equal protection and raise questions about whether algorithmic classifications can satisfy the test of reasonable classification under Article 14.

3.2. ARTICLE 19 AND THE CHILLING EFFECT OF ALGORITHMIC SURVEILLANCE

Article 19 of the Constitution guarantees fundamental freedoms including freedom of speech and expression, association, and movement. In the digital era, these freedoms are increasingly exercised through online platforms and digital communication channels. Cybercrime policing tools that rely on large-scale monitoring of online activity and communication metadata therefore directly implicate Article 19 rights Shreya (2015).

The Supreme Court has recognised that vague or overbroad state action in the digital sphere can produce a chilling effect on free expression, leading individuals to self-censor out of fear of legal consequences Shreya (2015). Algorithmic surveillance systems, which operate continuously and often invisibly, may create precisely such an environment. When individuals are uncertain about the criteria by which online behaviour is flagged as suspicious, the exercise of constitutionally protected freedoms becomes constrained.

While Article 19 permits reasonable restrictions in the interests of public order, security, and sovereignty, such restrictions must be proportionate and narrowly tailored. Algorithmic policing tools that engage in indiscriminate data collection or profiling risk exceeding these constitutional limits, particularly in the absence of clear statutory standards governing their deployment Anuradha (2020).

3.3. ARTICLE 21, DUE PROCESS, AND INFORMATIONAL PRIVACY

Article 21 forms the cornerstone of due process in Indian constitutional law. The Supreme Court has interpreted the right to life and personal liberty to include not only physical liberty but also dignity, autonomy, and privacy Maneka (1978), Puttaswamy v. Union of India, (2017). Any deprivation of liberty must therefore follow a procedure that is just, fair, and reasonable.

The recognition of privacy as a fundamental right has extended constitutional scrutiny to state practices involving data collection, surveillance, and profiling. In Justice (2017), the Court held that any state action infringing privacy must satisfy the tests of legality, legitimate aim, necessity, and proportionality. AI-driven cybercrime investigations, which depend on continuous processing of personal data and automated inference, must be assessed against this standard.

A critical concern under Article 21 is the dilution of the "reason to believe" standard in criminal investigations. Traditionally, investigative powers are exercised based on the independent application of mind by a human officer, subject to judicial oversight Ratanlal and Dhirajlal (2022). When suspicion is generated or significantly influenced by algorithmic systems, there is a risk that human judgment becomes secondary or symbolic. Such delegation of decision-making authority to opaque systems threatens procedural fairness and accountability.

3.4. INTERRELATIONSHIP OF ARTICLES 14, 19, AND 21 IN ALGORITHMIC POLICING

The Supreme Court has repeatedly emphasised that Articles 14, 19, and 21 must be read together when assessing the constitutionality of state action Maneka (1978). Algorithmic policing implicates all three provisions simultaneously by creating classifications that may be arbitrary, restricting digital freedoms through surveillance, and affecting personal liberty through automated suspicion.

This interrelationship is particularly significant in cybercrime investigations, where state action is often covert, data-driven, and technologically complex. The absence of transparency and explainability in algorithmic systems makes it difficult to assess compliance with constitutional requirements, thereby weakening the effectiveness of judicial review. As a result, algorithmic policing poses a structural challenge to the constitutional framework governing criminal justice in India.

This constitutional analysis provides the foundation for examining how algorithmic tools interact with statutory surveillance powers, evidentiary rules, and judicial oversight mechanisms, which is addressed in the next section.

4. STATUTORY FRAMEWORK GOVERNING CYBERCRIME INVESTIGATION AND ALGORITHMIC POLICING IN INDIA

While constitutional principles provide the normative foundation for evaluating algorithmic policing, the day-to-day deployment of AI in cybercrime investigations is governed by statutory law. In India, the primary legal instruments relevant to cybercrime investigation, surveillance, and digital evidence were enacted in a pre-algorithmic era. As a result, they neither expressly authorise nor adequately regulate the use of artificial intelligence in policing. This section critically examines the existing statutory framework and highlights its limitations in addressing algorithmic investigations.

4.1. INFORMATION TECHNOLOGY ACT, 2000 AND STATE SURVEILLANCE POWERS

The Information (2000) constitutes the principal statute governing cyber offences and electronic governance in India. Sections 43 and 66 of the Act criminalise unauthorised access, data theft, and related cyber offences, while Chapter XI provides investigative powers to the state. Of particular relevance to algorithmic policing are Sections 69, 69A, and 69B, which empower the government to intercept, monitor, decrypt, or block information in the interest of sovereignty, security, public order, and prevention of offences.

Although these provisions provide statutory backing for digital surveillance, they do not contemplate the use of artificial intelligence for automated monitoring or predictive analysis. The language of the Act assumes human-driven interception and decision-making, without addressing algorithmic inference, automated flagging, or machine-led pattern detection Bhatia (2021). This statutory silence creates ambiguity regarding the legality of AI-driven surveillance practices and weakens procedural safeguards.

Judicial scrutiny of Section 69 has emphasised the need for proportionality and procedural safeguards, particularly after the recognition of privacy as a fundamental right Puttaswamy v. Union of India, (2017). However, the absence of transparency

requirements or independent oversight mechanisms for algorithmic surveillance raises concerns about compliance with constitutional standards of necessity and proportionality Srikrishna (2023).

4.2. CRIMINAL PROCEDURE AND THE REQUIREMENT OF HUMAN JUDGMENT

Criminal investigation in India is traditionally governed by the Code of Criminal Procedure, which vests investigative discretion in police officers subject to statutory limits and judicial oversight. Concepts such as reasonable suspicion, reason to believe, and application of mind are embedded throughout the procedural framework. These requirements presuppose that investigative decisions are made by identifiable human actors who can be held accountable for their actions Ratanlal and Dhirajlal (2022).

Algorithmic policing complicates this structure by introducing non-human decision-making inputs that may significantly influence investigative outcomes. When AI systems generate risk assessments or identify potential suspects, the locus of decision-making shifts away from the investigating officer. This raises questions about whether procedural safeguards designed for human judgment can meaningfully operate in an algorithmic environment Citron (2008).

Moreover, criminal procedure law does not currently mandate disclosure of algorithmic processes or data sources used in investigations. As a result, accused persons may be denied the opportunity to challenge the basis of suspicion or surveillance, undermining principles of natural justice and fair trial.

4.3. INDIAN EVIDENCE ACT AND ADMISSIBILITY OF ALGORITHMIC OUTPUTS

The admissibility of electronic evidence in India is governed by Sections 65A and 65B of the Indian (1872). These provisions establish the conditions under which electronic records may be admitted as evidence, including certification requirements and assurance of authenticity. While these provisions address digital data, they do not explicitly consider algorithmically generated outputs such as predictive scores, similarity indices, or automated alerts.

Courts have traditionally treated electronic evidence as documentary evidence, subject to verification of source and integrity. However, algorithmic outputs involve additional layers of processing, modelling, and inference that are not easily captured within the existing evidentiary framework Casey (2019). Without access to information about how an algorithm functions, courts may struggle to assess reliability, accuracy, and probative value.

The risk is that algorithmic outputs may be accorded undue evidentiary weight due to their perceived objectivity, despite underlying biases or error rates. This concern is particularly acute in cybercrime cases, where technical complexity already places accused persons at a disadvantage Pasquale (2015).

4.4. DATA PROTECTION LAW AND STATE EXEMPTIONS

The enactment of the Digital (2023) marks a significant development in India's data governance framework. The Act establishes principles governing the collection, processing, and storage of personal data and imposes obligations on data

fiduciaries. However, the Act also contains broad exemptions for state action undertaken in the interest of security, sovereignty, and public order.

These exemptions significantly limit the Act's effectiveness as a safeguard against intrusive algorithmic policing. AI-driven cybercrime investigations often involve extensive data processing, profiling, and inference, activities that directly implicate informational privacy Srikrishna (2023). In the absence of stringent procedural requirements or independent oversight for state exemptions, data protection law offers limited protection against potential misuse of AI in policing.

4.5. REGULATORY GAPS AND THE NEED FOR LEGISLATIVE CLARITY

The existing statutory framework governing cybercrime investigation in India does not adequately address the challenges posed by algorithmic policing. Surveillance powers under the IT Act lack AI-specific safeguards, criminal procedure law assumes human judgment, evidentiary rules do not account for algorithmic inference, and data protection law provides broad exemptions to the state.

This regulatory gap allows AI-driven cyber policing to operate without clear legal boundaries, raising serious concerns about arbitrariness, accountability, and constitutional compliance. Without explicit legislative intervention, algorithmic policing risks becoming an extra-legal practice, shielded from meaningful judicial scrutiny and public accountability.

The next section examines how these statutory gaps interact with judicial oversight mechanisms and the challenges faced by courts in reviewing algorithmic investigations.

5. JUDICIAL OVERSIGHT AND THE CHALLENGES OF REVIEWING ALGORITHMIC INVESTIGATIONS

Judicial oversight functions as the primary safeguard against the abuse of investigative power in India's criminal justice system. Courts are entrusted with ensuring that state action complies with constitutional mandates of fairness, proportionality, and accountability. However, the increasing reliance on algorithmic tools in cybercrime investigations poses significant challenges to the traditional mechanisms of judicial review. These challenges arise from the technical complexity, opacity, and institutional unfamiliarity associated with artificial intelligence-based systems.

5.1. LIMITS OF TRADITIONAL JUDICIAL REVIEW IN ALGORITHMIC CONTEXTS

Indian courts have developed robust doctrines to review investigative action, including tests of arbitrariness under Article 14, proportionality under Articles 19 and 21, and procedural fairness under Article 21 Maneka (1978), Modern (2016). These doctrines assume that the decision-making process of the state is capable of being articulated, examined, and assessed against legal standards.

Algorithmic investigations complicate this assumption. AI systems often generate outputs without providing clear explanations of the underlying reasoning. When investigative decisions are influenced by machine-generated risk scores or

alerts, courts may find it difficult to ascertain whether constitutional requirements have been satisfied Wachter et al. (2017). The absence of intelligible reasoning undermines the ability of courts to determine whether a decision was arbitrary, disproportionate, or unsupported by evidence.

Moreover, judicial deference to executive expertise in matters of security and technology may further weaken scrutiny. Courts may be reluctant to question the validity of algorithmic tools deployed by law enforcement, particularly when such tools are presented as necessary for combating sophisticated cyber threats Pasquale (2015).

5.2. EVIDENTIARY CHALLENGES AND THE RIGHT TO FAIR TRIAL

The use of algorithmic tools in investigations raises significant concerns regarding the right to a fair trial. Article 21 encompasses not only protection against unlawful deprivation of liberty but also the right to a fair and reasonable procedure, including the opportunity to challenge evidence presented by the prosecution Zahira (2004).

Algorithmic outputs introduced as part of the investigative record may be difficult for accused persons to contest. The technical complexity of AI systems, coupled with the lack of disclosure regarding training data, model design, and error rates, places defendants at a structural disadvantage Citron (2008). Without access to this information, cross-examination and adversarial testing of evidence become largely illusory.

Indian evidentiary jurisprudence has not yet developed clear standards for assessing the reliability of algorithmic evidence. In the absence of such standards, courts risk either excluding potentially useful evidence due to uncertainty or, conversely, accepting algorithmic outputs at face value due to their perceived scientific neutrality. Both outcomes undermine the integrity of the judicial process Casey (2019).

5.3. PRIVACY JURISPRUDENCE AND PROPORTIONALITY REVIEW

The Supreme Court's privacy jurisprudence provides a potential framework for reviewing algorithmic investigations. In Justice (2017), the Court held that any infringement of privacy must satisfy a four-pronged test: legality, legitimate aim, necessity, and proportionality. This test requires courts to examine not only the existence of statutory authority but also the manner and extent of data collection and processing.

Applying this framework to algorithmic policing reveals significant gaps. While surveillance may be authorised under existing statutes, the necessity and proportionality of algorithmic data processing are rarely subjected to rigorous scrutiny. Courts are often not presented with sufficient information to assess whether less intrusive alternatives exist or whether data collection is narrowly tailored to specific investigative needs Srikrishna (2023).

5.4. INSTITUTIONAL CAPACITY AND THE KNOWLEDGE GAP

A critical but often overlooked challenge is the institutional capacity of the judiciary to engage with algorithmic systems. Judges are trained in legal reasoning,

not in machine learning or data science. Without adequate technical understanding or access to independent expertise, courts may struggle to meaningfully evaluate the functioning and implications of AI tools used in investigations Surden (2019).

The absence of court-appointed technical assessors or specialised procedures for reviewing algorithmic evidence exacerbates this problem. As a result, judicial oversight risks becoming formal rather than substantive, focusing on procedural compliance rather than examining the deeper constitutional implications of algorithmic decision-making.

5.5. NEED FOR RECALIBRATED JUDICIAL STANDARDS

The challenges outlined above indicate that existing modes of judicial review are ill-suited to the realities of algorithmic policing. To preserve constitutional accountability, courts must adapt their standards and procedures. This may include requiring disclosure of algorithmic logic and error rates, insisting on demonstrable human oversight, and developing jurisprudence on the admissibility and weight of algorithmic evidence Wachter et al. (2017), Pasquale (2015).

Without such recalibration, judicial oversight risks being outpaced by technological change. Algorithmic investigations may continue to shape outcomes in criminal cases without being subjected to the rigorous scrutiny that constitutional due process demands. The following section examines the broader ethical and accountability concerns raised by this shift and explores how they intersect with legal obligations in the Indian context.

6. ETHICAL AND ACCOUNTABILITY CONCERNS IN ALGORITHMIC CYBER POLICING

Beyond constitutional and statutory questions, the use of artificial intelligence in cybercrime investigations raises fundamental ethical concerns relating to accountability, legitimacy, and the moral limits of state power. Ethical analysis is particularly relevant in the Indian context, where the criminal justice system already grapples with issues of trust deficit, unequal enforcement, and institutional opacity. Algorithmic policing, if not carefully governed, risks deepening these concerns by obscuring responsibility and normalising intrusive forms of surveillance.

6.1. DIFFUSION OF RESPONSIBILITY AND THE ACCOUNTABILITY GAP

A core ethical challenge of algorithmic policing lies in the diffusion of responsibility. Traditional policing decisions are attributable to identifiable human actors, such as investigating officers or supervisory authorities, who can be held legally and institutionally accountable for misuse of power. Algorithmic systems disrupt this chain of accountability by introducing multiple actors, including software developers, data providers, vendors, and state agencies, none of whom may bear clear responsibility for adverse outcomes Pasquale (2015).

In cybercrime investigations, when an individual is flagged or subjected to surveillance based on algorithmic assessment, it becomes difficult to determine who is accountable for errors, bias, or rights violations. The investigating officer may rely on the algorithm, the vendor may claim proprietary secrecy, and the state may invoke national security justifications. This fragmentation undermines the

constitutional principle that coercive state action must be traceable to accountable decision-makers Citron (2008).

From an ethical standpoint, accountability is not merely a procedural requirement but a moral obligation tied to the legitimacy of state authority. The inability to assign responsibility for algorithmic decisions erodes public trust and weakens democratic oversight.

6.2. AUTOMATED SUSPICION AND THE PRESUMPTION OF INNOCENCE

The presumption of innocence is a foundational principle of criminal justice, implicit in Article 21 and repeatedly affirmed by Indian courts. Algorithmic policing challenges this principle by generating suspicion based on probabilistic assessments rather than concrete evidence of wrongdoing. Individuals may be subjected to monitoring, investigation, or coercive measures not because of past conduct but because an algorithm predicts future risk Barocas and Selbst (2016).

Such predictive logic raises ethical concerns about fairness and moral agency. Treating individuals as potential offenders based on statistical correlations reduces them to data points and undermines the idea that criminal liability must be grounded in voluntary human action. In the cybercrime context, where digital behaviour can be ambiguous and context-dependent, the risk of misinterpretation is particularly acute Wall (2018).

Ethically, the use of predictive tools blurs the line between prevention and punishment. When preventive surveillance becomes indistinguishable from investigative action, the moral justification for state intrusion becomes fragile.

6.3. CONSENT, AWARENESS, AND INFORMATIONAL ASYMMETRY

Ethical governance of data-driven systems requires meaningful consent and awareness. In algorithmic cyber policing, individuals are rarely informed that their data is being processed, profiled, or analysed by AI systems. This informational asymmetry deprives individuals of agency and undermines the ethical legitimacy of surveillance practices Floridi et al. (2018).

Although law enforcement activities often operate without consent, ethical standards still demand proportionality, necessity, and minimisation of harm. The routine and large-scale use of AI for monitoring digital behaviour risks normalising pervasive surveillance, even in the absence of specific suspicion. This raises concerns about dignity and autonomy, values that the Supreme Court has recognised as integral to Article 21 Puttaswamy v. Union of India, (2017).

6.4. TRANSPARENCY, EXPLAINABILITY, AND MORAL JUSTIFICATION

Transparency is not only a legal requirement but an ethical one. Decisions that affect individual liberty must be capable of being explained and justified. Algorithmic systems that operate as black boxes undermine this ethical expectation. When neither the individual nor the state can clearly explain why a particular person was flagged as suspicious, the moral legitimacy of investigative action is called into question Wachter et al. (2017).

Explainability also relates to fairness. Without understanding how an algorithm functions, it is impossible to assess whether it treats individuals equitably or systematically disadvantages certain groups. Ethical AI governance therefore requires that systems used in policing be intelligible to those who deploy them and subject to independent scrutiny.

6.5. ETHICAL GOVERNANCE AS A CONSTITUTIONAL IMPERATIVE

In the Indian constitutional framework, ethical concerns cannot be neatly separated from legal obligations. The Supreme Court has consistently emphasised that dignity, fairness, and reasonableness are integral to constitutional governance. Algorithmic policing that compromises these values risks violating not only ethical norms but also constitutional principles Seervai (2015).

Ethical governance of AI in cyber policing thus demands more than voluntary guidelines or aspirational principles. It requires enforceable norms that integrate ethical considerations into legal standards of accountability, transparency, and proportionality. Without such integration, algorithmic policing may erode the moral foundations of criminal justice and weaken public confidence in the rule of law.

The following section advances a set of legal and institutional reforms necessary to reconcile algorithmic cyber policing with constitutional due process and ethical accountability in India.

7. RECONCILING ALGORITHMIC POLICING WITH CONSTITUTIONAL DUE PROCESS: LEGAL AND INSTITUTIONAL REFORMS

The constitutional, statutory, and ethical analysis undertaken in the preceding sections demonstrates that algorithmic policing in cybercrime investigations cannot be evaluated through existing legal frameworks without significant recalibration. The challenge is not the mere use of artificial intelligence by law enforcement, but the manner in which such use redistributes decision-making power, obscures accountability, and dilutes established procedural safeguards. Reconciling algorithmic policing with constitutional due process therefore requires a combination of legislative clarity, judicial adaptation, and institutional reform.

At the legislative level, India urgently requires a clear statutory framework governing the use of artificial intelligence in criminal investigations. Existing provisions under the Information (2000) and criminal procedure laws confer broad surveillance and investigative powers but do not address algorithmic decision-making, automated profiling, or predictive assessments. In the absence of explicit authorisation and limits, the deployment of AI tools risks failing the legality requirement articulated by the Supreme Court under Article 21 Puttaswamy v. Union of India, (2017). A dedicated statutory framework should define permissible uses of AI in policing, specify the stages of investigation at which algorithmic tools may be employed, and prohibit fully automated decision-making in matters affecting personal liberty.

A core component of such regulation must be enforceable standards of transparency and explainability. While complete disclosure of algorithmic source code may not always be feasible due to security or proprietary concerns, constitutional due process requires that investigative decisions be capable of being

explained in intelligible terms. Courts cannot assess arbitrariness, proportionality, or necessity if the logic underlying suspicion remains opaque Wachter et al. (2017). Indian law must therefore mandate functional explainability, requiring law enforcement agencies to disclose the purpose, data sources, limitations, and error rates of algorithmic tools used in investigations. This aligns with the Supreme Court's insistence on reasoned state action under Articles 14 and 21 E et al. (1974), Maneka (1978).

Human oversight must also be legally reinforced as a constitutional necessity rather than treated as a procedural formality. Algorithmic tools should be confined to an assistive role, supporting but never substituting human judgment. Investigating officers must be required to independently apply their mind and record reasons when acting upon algorithmic outputs. This safeguard is essential to preserve the traditional requirement of "reason to believe," which serves as a bulwark against arbitrary investigation Ratanlal and Dhirajlal (2022). Without such safeguards, automation bias may result in investigative decisions being effectively delegated to machines, undermining procedural fairness and accountability Citron (2008).

Judicial oversight mechanisms must also evolve to address the realities of algorithmic policing. Courts play a central role in enforcing constitutional limits on state power, yet traditional modes of judicial review are ill-equipped to scrutinise complex AI systems. Indian courts should develop jurisprudential standards requiring disclosure of algorithmic reliance whenever investigative action is challenged. In appropriate cases, courts may rely on independent technical experts or court-appointed assessors to evaluate the reliability and fairness of algorithmic tools, thereby strengthening meaningful judicial review Surden (2019).

Evidentiary standards under the Indian Evidence Act must similarly be adapted. Algorithmically generated outputs used in cybercrime investigations should not be treated as neutral or self-validating evidence. Courts must require proof of reliability, accuracy, and relevance, and ensure that accused persons are afforded a genuine opportunity to challenge such material. Without adversarial scrutiny, the admission of algorithmic evidence risks undermining the right to a fair trial under Article 21 Zahira (2004), Casey (2019).

Data protection and privacy safeguards form another critical pillar of reform. Although the Digital (2023) establishes a general framework for data governance, broad exemptions granted to the state limit its effectiveness in the law enforcement context. To align with the proportionality test laid down in Puttaswamy, algorithmic cyber policing must be accompanied by strict data minimisation norms, purpose limitation, and retention controls. Large-scale or continuous surveillance through AI systems should be subject to heightened procedural safeguards, including prior authorisation and post-facto review Srikrishna (2023).

Finally, institutional accountability mechanisms must be strengthened. Independent audits of algorithmic tools used by law enforcement should be mandated to assess bias, accuracy, and compliance with constitutional standards. The diffusion of responsibility inherent in algorithmic systems cannot be allowed to shield the state from accountability. Constitutional governance demands that coercive power, even when technologically mediated, remain traceable to identifiable public authorities answerable to law Pasquale (2015).

Together, these reforms represent a shift from ad hoc technological adoption to constitutionally disciplined governance. They seek to ensure that artificial intelligence enhances investigative capacity without eroding the foundational values of fairness, equality, and liberty that underpin India's constitutional order.

8. CONCLUSION

Artificial intelligence has the potential to significantly augment India's capacity to combat cybercrime. However, the constitutional legitimacy of algorithmic policing cannot be assumed merely because such technologies promise efficiency or effectiveness. This paper has demonstrated that AI-driven cybercrime investigations raise profound concerns under Articles 14, 19, and 21 of the Constitution of India by introducing opaque decision-making, automated suspicion, and expansive digital surveillance into the criminal justice process.

The analysis reveals that algorithmic policing currently operates in a constitutional and regulatory grey zone. Existing statutes governing surveillance, criminal procedure, and digital evidence were not designed to accommodate machine-generated inference, while judicial oversight mechanisms face serious challenges in scrutinising opaque algorithmic systems. Without explicit safeguards, the use of AI risks diluting the requirement of reasoned suspicion, undermining equality before law, chilling constitutionally protected freedoms, and eroding procedural fairness.

The survival of due process in the age of algorithmic policing depends not on rejecting technology, but on subordinating it to constitutional discipline. Legislative clarity, enforceable transparency standards, meaningful human oversight, and recalibrated judicial review are essential to ensure that artificial intelligence remains a tool of governance rather than a substitute for constitutional accountability. In the absence of such measures, algorithmic efficiency may come at the cost of the very rule of law it seeks to protect.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Agarwal, S., and Choudhary, A. (2020). Cyber Crimes and Digital Policing in India. Eastern Book Company.

Angwin, J., Larson, J., Mattu, S., and Kirchner, L. (2016). Machine Bias. ProPublica.

Anuradha Bhasin v. Union of India, AIR (2020) SC 1308 (India).

Barocas, S., and Selbst, A. D. (2016). Big Data's Disparate Impact. California Law Review, 104(3), 671–732. https://doi.org/10.2139/ssrn.2477899

Bhatia, G. (2021). The Transformative Constitution: A Radical Biography in Nine Acts. HarperCollins India.

Casey, E. (2019). Digital Evidence and Computer Crime (3rd ed.). Academic Press.

Citron, D. K. (2008). Technological Due Process. Washington University Law Review, 85(6), 1249–1313.

Constitution of India. (1950). Articles 14, 19, and 21. https://doi.org/10.1080/10570315009373398

Crawford, K. (2021). Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press. https://doi.org/10.12987/9780300252392

Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).
E.P. Royappa v. State of Tamil Nadu, (1974) 4 SCC 3 (India).
Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Press.
Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An Ethical Framework for a Good AI Society. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
Hung, T. W. (2023). Predictive Policing and Algorithmic Fairness: Examining Legal and Ethical Challenges. Synthese, 201, 1–20. https://doi.org/10.1007/s11229-023-04189-0
Indian Evidence Act, 1872, §§ 65A–65B (India).
Information Technology Act, 2000, §§ 43, 66, 69, 69A, 69B (India).
Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. Sage Publications. https://doi.org/10.4135/9781473909472
Lum, K., and Isaac, W. (2016). To Predict and Serve? Significance, 13(5), 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x
Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).
MeitY. (2023). Annual report on Cyber Security and Cyber Crime. Ministry of Electronics and Information Technology, Government of India.
Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353 (India).
NITI Aayog. (2022). Responsible AI for All: A Framework for Ethical Artificial Intelligence. Government of India.
O'Neill, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing.
Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061
Ratanlal and Dhirajlal. (2022). The Code of Criminal Procedure (26th ed.). LexisNexis.
Seervai, H. M. (2015). Constitutional Law of India (4th ed.). Universal Law Publishing.
Selvi v. State of Karnataka, Air (2010) SC 1974 (India).
Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
Srikrishna, B. N. (2023). Framing a Data Protection Law for India: Privacy, Security and Governance. Oxford University Press.
Surden, H. (2019). Artificial Intelligence and Law: An Overview. Georgia State University Law Review, 35(4), 1305–1337.
Vats, A. (2022). The Problems with Predictive Policing. Information, Communication and Society, 25(4), 579–595.
Vidhi Centre for Legal Policy. (2021). Facial Recognition Technology in India: A Legal and Constitutional Analysis. Vidhi Centre for Legal Policy.
Wachter, S., Mittelstadt, B., and Russell, C. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
Wall, D. S. (2018). Cybercrime: The Transformation of Crime in the Information Age (2nd ed.). Polity Press.
Zahira Habibulla H. Sheikh v. State of Gujarat, (2004) 4 SCC 158 (India).