VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ALGORITHMIC POLICING IN CYBERCRIME INVESTIGATIONS: EXAMINING CONSTITUTIONAL SAFEGUARDS UNDER ARTICLES 14, 19 AND 21 OF THE INDIAN CONSTITUTION

- Ayushi Singh[1]

Abstract

The rapid digitization 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.[2] 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 .

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. 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.[3]

Keywords: National Security, Facial Recognition, Predictive modelling.

INTRODUCTION

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

[1] Student at Amity Law School, Amity University, Noida

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

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

such as reason to believe, proportionality, and procedural fairness . 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.

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. Even recent data protection legislation provides broad exemptions to the state, thereby limiting its effectiveness as a safeguard against intrusive surveillance practices.[4]

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.

[4] 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

2.1. 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)[5], 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.

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. 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 .

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

[5] Maneka Gandhi v. Union of India, (1978) 1 SCC 248 (India).

ability of affected individuals to understand, contest, or challenge decisions that adversely impact them . 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. 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 .[6]

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.

[6] 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

2.2. 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 [7]

2.3. 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 .[8]

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 . 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.[9]

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. Such outcomes challenge the constitutional mandate of equal protection and raise questions about whether algorithmic classifications can satisfy

[7] Seervai, H. M. (2015). Constitutional Law of India (4th ed.). Universal Law Publishing.

[8] Ratanlal and Dhirajlal. (2022). The Code of Criminal Procedure (26th ed.). LexisNexis.

[9] O'Neill, C. (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing.

the test of reasonable classification under Article 14.

2.4. 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.[10]

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.[11] 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.

2.5. 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. 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

[10] Srikrishna, B. N. (2023). Framing a Data Protection Law for India: Privacy, Security and Governance. Oxford University Press.

[11] Surden, H. (2019). Artificial Intelligence and Law: An Overview. Georgia State University Law Review, 35(4), 1305–1337.

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. 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.

2.6. 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.[12]

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.[13]

CONCLUSION

The increasing use of algorithmic policing in cybercrime investigations has transformed the manner in which law enforcement agencies detect, predict, and prevent digital offences in

[12] Vats, A. (2022). The Problems with Predictive Policing. Information, Communication and Society, 25(4), 579–595.

[13] Selvi v. State of Karnataka, Air (2010) SC 1974 (India). Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

India. While these technologies enhance efficiency, speed, and data analysis capabilities, they also raise significant constitutional concerns relating to equality, freedom, and privacy. The study demonstrates that the deployment of predictive algorithms, facial recognition systems, and automated surveillance mechanisms may lead to discriminatory profiling, lack of transparency, and arbitrary state action, thereby affecting the guarantees enshrined under Articles 14, 19, and 21 of the Indian Constitution. Article 14 requires fairness and non-arbitrariness in state actions, yet biased datasets and opaque algorithms may perpetuate unequal treatment. Similarly, excessive digital surveillance can create a chilling effect on free speech and expression protected under Article 19. Most importantly, the right to privacy and personal liberty under Article 21, as recognised in the Justice K.S. Puttaswamy v. Union of India judgment, demands procedural safeguards, accountability, and proportionality in technological policing practices. Therefore, India must adopt a balanced regulatory framework that ensures technological advancement while safeguarding constitutional rights and democratic values in cybercrime investigations.

REFERENCES

1. Joshi, Pratyaksh & Wamankar, Yogesh, "Algorithmic Policing and Due Process in Cybercrime Investigations: A Constitutional Analysis under Articles 14, 19 and 21 of the Indian Constitution," *ShodhSamajik: Journal of Social Studies*, Vol. 2, No. 2, 2025.
2. Barocas, Solon & Selbst, Andrew D., "Big Data's Disparate Impact," *California Law Review*, Vol. 104, No. 3, 2016.
3. Citron, Danielle Keats, "Technological Due Process," *Washington University Law Review*, Vol. 85, No. 6, 2008.
4. Crawford, Kate, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, 2021.
5. Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.
6. Narayan, Shivangi, *Predictive Policing and the Construction of the "Criminal": An Ethnographic Study of Delhi Police*, Springer Nature, 2023.
7. Lum, Kristian & Isaac, William, "To Predict and Serve?," *Significance Magazine*, Vol. 13, No. 5, 2016.
8. Sambasivan, Nithya et al., "Non-portability of Algorithmic Fairness in India," *Proceedings of FAT* Conference, 2020.
9. Sambasivan, Nithya et al., "Re-imagining Algorithmic Fairness in India and Beyond," *Proceedings of FAT* Conference, 2021.
10. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 — Supreme Court of India decision recognising the right to privacy as a fundamental right under Article 21.