



LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

[ISSN: 2583-7753]

Volume 4 | Issue 3

2026

DOI: <https://doi.org/10.70183/lijdlr.2026.v04.291>

© 2026 LawFoyer International Journal of Doctrinal Legal Research

Follow this and additional research works at: www.lijdlr.com

Under the Platform of LawFoyer – www.lawfoyer.in

After careful consideration, the editorial board of LawFoyer International Journal of Doctrinal Legal Research has decided to publish this submission as part of the publication.

In case of any suggestions or complaints, kindly contact (info.lijdlr@gmail.com)

To submit your Manuscript for Publication in the LawFoyer International Journal of Doctrinal Legal Research, To submit your Manuscript [Click here](#)

REGULATING AI MONOPOLIES IN CRIME DETECTION MECHANISM

Diana Das¹

I.ABSTRACT

Artificial Intelligence is increasingly being integrated into crime detection through predictive policing, facial recognition, crime-mapping, cyber-surveillance and financial fraud detection systems. While these technologies may enhance efficiency, speed and pattern recognition in law enforcement, their concentration in the hands of the State and a limited number of private technology vendors creates a distinct form of “AI monopoly” in criminal justice. This paper examines AI monopoly not merely as economic market dominance, but as functional control over data, algorithms and institutional policing infrastructure. The study aims to analyse the operational role of AI in contemporary crime detection, critically assess the impact of monopolised AI systems on investigation and surveillance practices, and propose regulatory safeguards to ensure accountability. Adopting a doctrinal and analytical approach, the paper evaluates the interaction between AI-driven policing and constitutional principles of equality, liberty, privacy, due process and procedural fairness. It argues that monopolised crime-detection technologies may reproduce historical bias, create feedback loops of over-policing, obscure decision-making through black-box algorithms and reduce the scope for independent human judgment. The paper further identifies the absence of a specific legal framework governing AI-based policing as a major regulatory gap. It recommends a rights-oriented accountability model based on data transparency, independent auditability, responsible data governance, human-in-the-loop decision-making, judicial oversight and statutory safeguards. Finally, the paper argues that constitutional values such as non-discrimination, privacy, fairness and due process must be embedded into the design, deployment and review of AI systems so that technological efficiency does not override the humane and constitutional foundations of criminal justice.

II.KEYWORDS

¹ 3rd Year, 6th Semester, 3 Years LL.B. (2023-2026), National Law University Odisha (India). Email: diana.das456@gmail.com

Artificial Intelligence; AI Monopoly; Predictive Policing; Algorithmic Accountability; Facial Recognition.

III.INTRODUCTION

Artificial Intelligence is gradually becoming a part of every regulation. Tools such as Predictive Policing software, Facial Recognition System, and Crime- mapping technologies are used by crime detecting departments for various purposes, such as crime detection in certain areas, analysing the pattern of crime, allocating Officers and to identify potential suspects. These systems are usually seemed to be efficient and impartial. But there are significant legal issues with their increasing dominance over criminal justice decisions.

The concept of AI Monopoly refers to the control over Data, Algorithms and Institutional Procedure rather than market supremacy. When law enforcement organisations rely heavily on a narrow range AI system, especially those crested with confidential algorithms and unique data, these technologies start to have big impact on how crime is detected, classifies and dealt with. Algorithmic evaluation might eventually take centre stage in determining surveillance tactics, which might limit the opportunity for critical analysis and independent human judgement.

There are major concerns associated with the technological power. AI system trained on historical crime data may repeatedly flag certain neighbourhoods or communities as “High Risk”, leading to over-policing and increased surveillance in those areas. These results frequently lead to feedback loops, in which increased crime detection activity result in more crime being reported, which in turn validates the system’s presumptions. However, many AI technologies opacity limits accountability by making it hard to comprehend or question how these judgements are arrived at.

This paper focuses at how the prevalence of AI in crime detection interacts with criminal justice principles, constitutional protections, and regulatory accountability with the larger framework of AI and Law.

The main issue is the that isn’t a clear legal framework that can govern AI- driven policing while upholding procedural justice, equality, and liberty.

A. Research Objectives

1. To examine the operational function of AI in contemporary crime detection mechanism.
2. To critically analyse the impact of AI monopoly on crime detection and investigation process.
3. To examine and propose regulation for AI monopolies.

B. Research Questions

1. What is the function of AI in across different sectors of crime detection system?
2. What are the impacts of AI monopolies on crime detection and investigation process?
3. How AI monopolies in crime detection be effectively regulated?

C. Research Methodology

This paper adopts a doctrinal and analytical research methodology to examine the regulation of AI monopolies in crime detection mechanisms. The study primarily relies on legal and policy materials, including constitutional principles, statutory frameworks, judicial precedents, regulatory guidelines and institutional reports relating to artificial intelligence, data protection, policing and criminal justice. Secondary sources such as academic commentaries, books, journal articles and expert reports are also used to understand the broader socio-legal implications of AI-driven crime detection. The paper analyses the role of predictive policing, facial recognition, crime-mapping and other AI-based tools in law enforcement, with particular focus on their impact on equality, privacy, liberty, due process and accountability.

It further undertakes a comparative examination of regulatory developments in India, the European Union and the United Kingdom to identify suitable safeguards against data monopoly, algorithmic opacity and excessive institutional dependence on private AI vendors. The methodology is qualitative in nature and aims to develop a rights-oriented regulatory framework based on transparency, auditability, human oversight, judicial supervision and constitutional-values-by-design.

IV.CONCEPTUAL FRAMEWORK

Artificial Intelligence (AI) is basically a tool or in simple words the competency of the machine to do activity, which typically require Human Mind. Essentially, artificial intelligence gives computer programs the ability to reason, understand, learn, and make decisions similarly to people.

A. Understanding AI Monopoly in Legal Governance

Under the conventional legal paradigm, monopoly is usually understood as economic control over a market. However, in AI-based legal governance, monopoly assumes a broader form of functional dominance over data, algorithms and institutional infrastructure. Within the criminal justice system, an AI monopoly may therefore arise where law enforcement becomes dependent on a limited set of AI systems or private vendors for surveillance, risk assessment, suspect identification and crime-mapping. Such dominance affects not only market competition but also the manner in which State power is exercised against individuals.

The European Union's current regulatory position is no longer confined to the European Commission's 2020 White Paper. It is now codified in the EU Artificial Intelligence Act, Regulation (EU) 2024/1689, which entered into force on 1 August 2024 and adopts a risk-based regulatory model. The Act is directly relevant to crime detection because it prohibits certain forms of predictive policing based on profiling and classifies several law-enforcement AI systems as high-risk, including systems used for assessing the risk of offending or reoffending, evaluating evidence reliability, profiling in criminal investigations, and supporting law enforcement authorities. These provisions show that AI used in criminal justice requires strict legal safeguards, including data-quality controls, transparency, risk mitigation and human oversight.

Accordingly, the concept of AI monopoly in crime detection must be understood not merely as technological concentration, but as concentrated control over legally consequential decision-making processes.² This shift moves the focus from commercial market share to the control of legal outcomes, administrative discretion, and policing strategies, fundamentally altering the way justice is administered.

² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

This contemporary monopoly can be defined by three dimensional:

1. **Data Monopoly**, which is defined as the exclusive reliance of AI system on pre-existing data sets that are beyond public scrutiny, such as the exclusive right to access and use surveillance data in the classification of crime.
2. **Algorithmic monopoly**, can be defined as the exclusive reliance of AI system on propriety algorithms known as “black box” system that are used as the primary means if assessing risk. By keeping the workings of the algorithms beyond the scrutiny of the judiciary, such algorithms effectively monopolise the process that are otherwise subject to the accountability of human actions.³
3. **Infrastructure Monopoly** can be defined as the integration of AI systems with the very fabric of law enforcement institutions, which leads to the creation of state dependency where the very capacity of the state to manage crime effectively is inextricably linked to the capacity of the technology itself.

Furthermore, increasing ‘State reliance on private AI’ vendors intensify these concerns.

V. AI IN CRIME DETECTION

Artificial Intelligence plays a crucial role in the detection of crime by acting as a high-speed analytical layer over traditional methods of law enforcement. At its core, Artificial Intelligence is a pattern recognition tool, and surveillance technologies have moved beyond mere recording to active monitoring.

1. **AI in Financial sector:** In the financial industry, AI is used for fraud detection and prevention. The machine learning algorithms analyse the transactions and check for abnormal patterns in spending, such as sudden large transactions, irregular spending patterns, and complex routing of funds. Network analysis is also used for detecting links between accounts used for money laundering. Such as Money laundering, Insider Trading or credit card frauds.
2. **AI in Cybersecurity:** AI-based cyber security systems are designed to track the

³ Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).

activities of the network and the user. Intrusion Detection Systems (IDS) are designed to detect the normal behaviour of the system. Any abnormal behaviour may be an indication of hacking. AI is also useful in detecting malware by identifying the patterns of the codes. Such as Hacking, phishing, cyber-extortion etc.⁴

3. AI in law enforcement and Investigations: Law enforcement organizations use AI for predictive policing, facial recognition, and crime pattern analysis. Predictive policing makes use of past crime statistics for predicting areas of high crime risk, and facial recognition technology matches images from surveillance systems with criminal records. AI detect crimes like theft, identification of suspect, etc.

4. AI in social media and Digital platform: Through the use of Natural Language Processing (NLP) and image recognition, AI systems can function as a digital sentry, constantly monitoring online content to identify harmful behaviours and coordinated criminal activities. These systems can be integrated to identify advanced cyberbullying by analysing sentiment and predatory language in real-time, while simultaneously recognizing online fraud and scams by analysing communication patterns and synthetic media usage in phishing activities. Moreover, by recognizing extremist keywords and radicalization markers, along with illegal images, AI can provide law enforcement with a powerful tool to counter the dissemination of extremist or illegal content and dismantle organized criminal activities before they can get out of hand.

VI.IMPACT OF AI MONOPOLIES IN CRIME DETECTION

1. AI monopolies as Data and Knowledge control: This concentration of massive data sets under the jurisdiction of the State or a handful of private technology companies can be seen as a kind of epistemic monopoly wherein the definition of "crime" no longer relies on any objective measurement of legality but instead relies

⁴ National Institute of Standards and Technology, *Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST Special Publication 800-94).

upon the interpretation of algorithmic logic. This kind of representation of data wherein certain crimes are brought to the surface while others remain hidden from view creates a kind of dependency for law enforcement agencies.

2. Impact on Crime Detection Mechanisms: When AI systems are trained on monopolized data sets, which contain historical, social, or institutional biases, they not only observe crime; they also shape and distort its perceived reality. Since AI systems are based on past police data, they end up creating a "feedback loop" where some communities are overrepresented as "high-risk" based on past over-policing, rather than actual crime rates. In contrast, some affluent or less-monitored areas remain underrepresented or completely disregarded, creating "blind spots" in our criminal justice system. This monopolized data set ends up creating a "prejudice" on the objective reality of crime distribution, replacing it with a data-driven prejudice that further fuels inequality.⁵

3. Algorithmic Reinforcement: The further reinforcement of these biases creates a recursive loop in which AI is no longer merely a neutral detection device but an active architect in the creation of the perception of crime. A monopoly-controlled AI, in identifying a particular area as "high-risk" based on biased historical data, sets off a wave of further policing in the area, which in turn guarantees a further increase in the overall number of arrests and incidents in a particular area. This is then fed back into the system, reinforcing the same part of the AI's dataset but with ever-higher "risk" scores. This is a self-fulfilling technology where the AI does not merely witness crime but is, in fact, an active architect in the creation of its own recording, thereby creating a skewed reality that justifies further surveillance and ignores the social complexities of the situation⁶.

VII. REGULATING AI MONOPOLIES IN CRIME DETECTION

AI systems play an increasingly significant role in policing decisions; therefore, there is

⁵ Andrew Guthrie Ferguson, *The Rise of Big Data Policing* (NYU Press 2017).

⁶ European Union Agency for Fundamental Rights, *Bias in Algorithms and AI* (2022).

an urgent need to develop a clear framework for algorithmic accountability. In India, this discussion must now be situated against the MeitY India AI Governance Guidelines, 2025, unveiled under the IndiaAI Mission. These Guidelines adopt a principles-based approach to responsible AI governance and emphasise “Do No Harm,” innovation sandboxes, risk mitigation, human-centric AI, transparency and accountability. However, their framework remains sector-agnostic and non-legislative, which limits their direct enforceability in the criminal justice context.

This limitation is important because law-enforcement AI is not an ordinary administrative technology. Predictive policing, facial recognition, crime-mapping and suspect-identification tools directly affect liberty, privacy, equality and due process. Therefore, the general principles contained in the MeitY Guidelines should be treated as a starting point, not as a complete regulatory answer. For crime detection, India requires sector-specific supplementation through binding rules that prescribe when AI may be used, what datasets may be relied upon, how bias and error rates must be audited, and how affected persons may challenge AI-assisted decisions.⁷

Accordingly, the regulation of AI monopolies in crime detection should combine the MeitY Guidelines’ broad principles with a dedicated statutory framework for policing AI. Such a framework must require prior risk assessment, transparent procurement, independent algorithmic audits, mandatory human oversight, explainability obligations for vendors, periodic review by an independent authority, and judicially enforceable safeguards wherever AI outputs influence investigation, surveillance or prosecution. This approach would ensure that India’s current AI governance position is meaningfully adapted to the special constitutional risks of criminal justice, rather than leaving policing technologies to executive discretion or private vendor control.

This has given rise to a situation where decisions regarding an individual’s liberty may be impacted, to some extent, by systems that are neither transparent nor legally accountable for their decisions. Algorithmic accountability will ensure that such systems are held accountable for clear legal mandates, including documentation

⁷ Ministry of Electronics and Information Technology, India AI Governance Guidelines, 2025, unveiled under the IndiaAI Mission on 5 November 2025.

regarding how they function, what data they utilize, and what reasoning they apply to decision-making processes.

1. Data Transparency and Auditability

A major step towards the regulation of such technologies is to ensure that they are transparent and can be audited. There are many policing technologies that are essentially "black boxes," in that even those who are using them may not entirely know how they are coming to a certain decision. There is a need for mandatory audit mechanisms to be in place, either through a regulatory agency or a court-supervised process, to determine whether or not these technologies are working in a fair and unbiased manner. Transparency may not necessarily mean that the technology itself is revealed to the general public, but that there is adequate information available for such a process.

2. Regulating Data

As the reliability of AI depends on the reliability, legality and representativeness of the data on which it is trained, data governance must form a central part of any regulatory framework for AI-based crime detection. This includes clear standards on how crime data is collected, classified, stored, reviewed and used, so that historical policing bias is not reproduced through automated systems. In India, this concern must now be examined not only through the Digital Personal Data Protection Act, 2023, but also through the Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology in November 2025.

These Rules operationalise important obligations relating to notice, consent-linked transparency, security safeguards, breach response, grievance redressal and data retention. They require notice to be clear and capable of enabling informed consent, and also require mechanisms through which individuals may exercise their statutory rights and make complaints to the Data Protection Board.

The Rules are particularly relevant to AI policing because they address retention and accountability. Rule-based retention obligations require personal data and processing logs to be retained for specified periods and erased thereafter unless further retention is legally required. This is significant for crime-detection AI because outdated, excessive or

irrelevant data may distort risk assessment and intensify surveillance against particular communities. The Rules also strengthen breach accountability by requiring safeguards, monitoring, investigation and remediation of unauthorised access.

Further, the constitution of the Data Protection Board of India creates an institutional mechanism for enforcing data protection duties. Therefore, data used in AI-based policing should not become an independent source of monopoly power; it must remain subject to legality, purpose limitation, retention limits, auditability, breach notification duties and independent regulatory oversight.⁸

3. Human Oversight

However, despite the efficiency of AI, the importance of human decisions should not be compromised. The introduction of the 'human-in-the-loop' requirement makes sure that the results and outputs provided by AI systems are not used in a decisive manner. The law enforcement agencies should critically evaluate the suggestions provided by AI systems and should not blindly accept them. This is especially true in the criminal justice system, as the consequences of the decision can have a significant impact on the rights and freedoms of individuals.

4. Judicial Oversight and statutory safeguard

There is a need for regulation, which should be backed by judicial oversight and legislation. In this case, there should be a system whereby the judiciary is empowered to review the use of AI in policing, especially in situations where there is an algorithmic outcome in the investigation or prosecution of a case⁹. This will include the power to request disclosure of relevant information about AI, especially in situations where it is essential for a fair trial.

Moreover, there should be legislation defining the permissible boundaries of AI use in law enforcement, particularly where such technologies involve surveillance, biometric identification, risk assessment or automated investigative prioritisation. Such legislation

⁸ Organisation for Economic Co-operation and Development, *OECD Principles on Artificial Intelligence* (2019).

⁹ The Digital Personal Data Protection Act, 2023 read with the Digital Personal Data Protection Rules, 2025.

must ensure that AI deployment is backed by law, pursues a legitimate State aim, and satisfies the requirement of proportionality so that technological advancement does not override constitutional justice. The appropriate Indian authority for this proposition is *Justice K.S. Puttaswamy v Union of India*, where the Supreme Court recognised privacy as a fundamental right and held that State intrusion must satisfy legality, necessity and proportionality. This framework is directly relevant to AI-enabled policing because facial recognition, predictive policing and data-driven surveillance may seriously affect privacy, liberty and due process.¹⁰

5. Judicial Precedents

- **Bridges v. South Wales Police (2020):** The use of automatic facial recognition technology by the South Wales Police was held to be unlawful by the Court of Appeal. The court held that there was insufficient legal guidance on where to use AFR technology and whom to put on a watchlist, as there was insufficient law to prevent bias and violation of privacy.¹¹

VIII. RECOMMENDATIONS AND WAY FORWARD

1. **Establishing clear legal principles for AI Regulations:** A well-structured response to the problem of AI monopolies in crime detection would start with the development of well-defined legal principles for the use of AI in criminal justice. Such principles would be based on the values of the constitution, such as equality, fairness, transparency, and accountability. The use of AI would be governed by the principles of necessity and proportionality to ensure the use of AI is only justified when necessary and to the least extent possible without infringing the rights of individuals.
2. **Strengthening Institutional Check on AI Vendors:** One of the biggest concerns is the increased dependency on private tech companies for policing tools and equipment, and this is where strict institutional control needs to be enforced. For this, it is important that the government puts in place strict checks and balances for all tech companies that supply AI equipment and tools to the police department. It is

¹⁰ *Justice K.S. Puttaswamy v Union of India* (2017) 10 SCC 1.

¹¹ *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

important that transparency is made mandatory in each and every contract signed by tech companies, so they have to be open and honest about how their equipment works, how it is limited, and how it might cause potential risks. It is also important that audits be conducted on this equipment to make sure it is not biased or discriminatory in any way. By doing this, we can make sure that private companies do not become responsible for police work and that the government is always answerable to its citizens.

3. Judicial Enforcements: For there to be effective regulation of AI technology used for crime detection, it is also essential that these legal bodies be able to comprehend and scrutinize these technologies. From the current situation, it is very obvious that there is a technical knowledge gap within these judicial and law enforcement oversight bodies, as well as within the minds of these legal practitioners. This, therefore, implies that there is a need for capacity building within these bodies and minds. This can be achieved by ensuring that these bodies and minds are technically educated and that technical experts are included within the judicial process.¹¹

4. Integration of Constitutional Values into AI: However, in order for such a regulation to be effective, it is essential that it extends beyond the mere deployment of the technology and starts getting involved in the actual design and development of the technology. This is called "Privacy and Ethics by Design," wherein values such as non-discrimination, privacy, and due process, which are embedded in the constitution, are directly incorporated into the "fabric" of this technology¹². This means that the programming sets for this technology must be carefully curated so that all the historical prejudices are stripped out, and this technology is designed in a way that certain groups of people are not targeted in a disproportionate way so that their rights are not violated in any way, even before it is handed over to law enforcement agencies.

The regulatory framework for AI monopolies in crime detection must be strengthened by incorporating recent legal developments on artificial intelligence and data protection. The EU Artificial Intelligence Act, Regulation (EU) 2024/1689, is particularly relevant because

it treats several law-enforcement AI systems as high-risk, including systems used for crime-risk assessment, evaluating evidence reliability, predicting reoffending, and profiling in criminal investigations. It also restricts certain biometric and predictive policing uses, thereby demonstrating that AI-based policing requires prior legal authorisation, risk assessment, transparency, human oversight and fundamental-rights safeguards.

In the Indian context, the Digital Personal Data Protection Act, 2023, read with the Digital Personal Data Protection Rules, 2025, provides an important foundation for regulating the personal-data dimension of AI-based crime detection. Since policing AI often depends on personal data, biometric data, surveillance records and behavioural patterns, data protection principles such as lawful processing, purpose limitation, notice, security safeguards and breach accountability become essential to prevent excessive data concentration. The DPDP Rules, 2025 were notified by the Government of India in November 2025 and operationalise the statutory framework under the DPDP Act. Further, India's AI Governance Guidelines released by MeitY under the IndiaAI Mission provide a contemporary policy basis for responsible AI adoption.

These guidelines emphasise safe, inclusive and responsible AI use, and they should be adapted specifically to criminal justice because policing involves direct consequences for liberty, privacy and equality. A sector-specific framework for AI in crime detection should therefore include mandatory algorithmic impact assessments, independent audits of datasets, explainability obligations for vendors, periodic review of error rates, safeguards against discriminatory outcomes, and clear rules preventing police authorities from relying solely on automated outputs.

Accordingly, the paper should recommend that India move from a general technology-governance model to a rights-sensitive policing-specific AI framework. Such a framework must require transparent procurement of AI tools, judicially reviewable deployment standards, human-in-the-loop decision-making, and constitutional-values-by-design. This would ensure that AI is used only as an assistive investigative tool and not as a substitute for legal reasoning, human discretion or judicial accountability.

IX.CONCLUSION

The incorporation of AI into the criminal justice system is a paradox that, on one

hand, provides unprecedented efficiency in crime mapping and predictive policing, but on the other, threatens to undermine the very pillars of due process and equal justice. As discussed throughout this paper, the creation of "AI Monopolies" that rely on a handful of unexplainable algorithms for surveillance and suspect detection threatens to turn historical prejudices into technological imperatives. When law enforcement is forced to rely on "black box" technologies, the ability for independent human judgment and critical thought is perilously diminished.

In order to break the feedback loops of over-policing and discrimination, the current legal paradigm must change from a reactive form of regulation to a more active "Privacy and Ethics by Design" mandate. This means stripping historical prejudices from datasets and ensuring that technical expertise is incorporated into judicial oversight bodies. The end result is one where the "humane element" of the law is supreme. As we continue to build toward a more technologically driven form of law, our dedication to constitutional precepts such as

non-discrimination, privacy, and due process must be as sophisticated as the technology used.

X. REFERENCES

1. Jaiswal A and Mishra PC, 'Artificial Intelligence (AI) and Criminal Justice System: Potential Benefits and Risks' (2023) 4(2) ShodhKosh: Journal of Visual and Performing Arts 3693
2. Pooja Agrawal, 'Algorithmic Bias in Artificial Intelligence: A Socio-Legal Perspective' (2024) *Global Insights Journal*
3. 'Artificial Fairness? Trust in Algorithmic Police Decision-Making' (2023) *Journal of Experimental Criminology*
4. NITI Aayog, *Responsible AI for All* (2021)
5. European Union Agency for Fundamental Rights, *Artificial Intelligence and Fundamental Rights* (2020)
6. Law Commission of India, Report No 245 (2014)

7. Law Commission of India, Report No 262 (2015)
8. National Institute of Standards and Technology, *Guide to Intrusion Detection and Prevention Systems (SP 800-94)*
9. Alexander Babuta and Marion Oswald, *Data Analytics and Algorithmic Bias in Policing* (2019) Royal United Services Institute