VOLUME 6 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ALGORITHMIC POLICING – CONCEPTS, TOOLS, AND GLOBAL PRACTICES

- Riya Sharma[1]

If the preceding chapter sought to understand the architecture of power in the digital age, the present one turns to its most tangible manifestation within law enforcement: algorithmic policing. It is here—at the intersection of code, data, and coercive authority—that abstract concerns begin to crystallize into concrete practices.[2]

Algorithmic policing is often introduced through the language of innovation. Efficiency is foregrounded. Objectivity is implied. The suggestion—sometimes explicit, often subtle—is that technology can correct the inconsistencies and biases that have long characterized human decision-making.[3] Yet, as this chapter will demonstrate, such optimism requires careful qualification.

For while algorithms may process information with remarkable speed, they do not exist outside the social and institutional contexts that shape their design. They inherit assumptions. They reflect priorities. And, at times, they reproduce the very inequities they are purported to eliminate.[4]

1.1 Meaning and Scope of Algorithmic Policing

Defining algorithmic policing is not a straightforward task. The term encompasses a range of technologies and practices, each differing in scope, complexity, and application. At its core, however, it refers to the use of computational systems—particularly those based on machine learning and statistical modeling—to assist or influence policing decisions.[5]

These systems operate by identifying patterns within data. Historical crime records, demographic information, geospatial data, and behavioral indicators are analyzed to generate

[1] Student at Amity Law School, Amity University, Noida
[2]Ferguson, The Rise of Big Data Policing (2017).
[3]O'Neil, Weapons of Math Destruction (2016).
[4]Barocas & Selbst (2016).
[5]Ferguson (2017).

insights—sometimes descriptive, sometimes predictive.[6] The outputs may inform decisions about patrol allocation, suspect identification, or risk assessment.

Yet, the scope of algorithmic policing extends beyond mere assistance. In certain contexts, algorithmic outputs acquire a form of authority. They are treated not simply as tools, but as recommendations imbued with a degree of epistemic weight.[7] This subtle shift—from aid to influence—marks a critical point of transition.

Because once algorithmic outputs begin to shape decisions, the question is no longer whether technology is being used, but how much it is being trusted.

1.2 Types of Algorithmic Policing

1. Predictive Policing

Predictive policing represents perhaps the most widely discussed application of algorithmic systems in law enforcement. It involves the use of historical data to forecast where crimes are likely to occur or who might be involved.[8]

At first glance, the logic appears intuitive. If certain areas have experienced higher crime rates in the past, it may be efficient to allocate resources accordingly. However, this reasoning is complicated by the nature of the data itself.

Crime data does not merely reflect criminal activity; it reflects policing patterns. Areas subjected to more intensive surveillance are likely to generate more recorded incidents, regardless of underlying crime rates.[9] When such data is fed into predictive models, the result may be a feedback loop—more policing leads to more data, which in turn justifies further policing.

Thus, prediction, rather than neutral, becomes self-reinforcing.

2. Facial Recognition Systems

[6]Lum & Isaac (2016).
[7]Pasquale, The Black Box Society (2015).
[8]Lum & Isaac (2016).
[9]Ferguson (2017).

Facial recognition technology (FRT) represents another significant dimension of algorithmic policing. These systems analyze facial features captured through images or video footage and compare them against existing databases to identify individuals.[10]

The potential applications are extensive—locating missing persons, identifying suspects, monitoring public spaces. Yet, the technology is not without controversy.

Accuracy rates vary. Studies have shown that certain systems perform less reliably when identifying individuals from marginalized communities, particularly women and persons with darker skin tones.[11] This disparity raises serious concerns about misidentification and its consequences.

Moreover, the deployment of FRT in public spaces introduces broader questions about surveillance. When identification becomes instantaneous and pervasive, anonymity—a cornerstone of public freedom—begins to erode.[12]

3. Risk Assessment Tools

Risk assessment tools are used to evaluate the likelihood that an individual will engage in criminal behavior or reoffend. These systems often draw upon a range of variables—criminal history, socio-economic background, behavioral indicators—to generate a risk score.[13]

Such tools are frequently used in decisions relating to bail, sentencing, and parole. Their appeal lies in their promise of consistency and objectivity. However, this promise is not always realized.

The variables used in these models are often proxies for deeper structural inequalities. Factors such as neighborhood, employment status, or educational background may correlate with risk scores, but they also reflect broader socio-economic disparities.[14]

As a result, risk assessment tools may inadvertently perpetuate systemic inequalities, embedding them within ostensibly neutral frameworks.

[10]Garvie, Bedoya & Frankle (2016).
[11]Joy Buolamwini & Timnit Gebru (2018).
[12]Solove (2008).
[13]Angwin et al. (2016).
[14]Barocas & Selbst (2016).

1.3 Working of Algorithms in Policing

To understand the implications of algorithmic policing, it is necessary to briefly consider how these systems function.

At a fundamental level, algorithms process input data to generate output predictions. This process involves training models on historical datasets, identifying patterns, and applying those patterns to new data.[15] Machine learning systems, in particular, refine their outputs over time, adjusting based on feedback.

However, this process is far from purely mechanical.

Decisions are made at every stage—what data to include, how to clean it, which variables to prioritize, what thresholds to set.[16] These decisions shape the behavior of the system, often in ways that are not immediately visible.

Furthermore, the complexity of certain models—particularly those based on deep learning—renders them difficult to interpret. Even those who design the systems may not fully understand how specific outputs are generated.[17] This opacity raises significant concerns about explainability and accountability.

1.4Global Practices and Case Studies

The adoption of algorithmic policing is not confined to any single jurisdiction. Across the world, governments have experimented with various forms of data-driven law enforcement, each reflecting distinct legal, social, and political contexts.

In the United States, predictive policing tools such as COMPAS and PredPol have been widely deployed.[18] While these systems have been praised for improving efficiency, they have also faced significant criticism for reinforcing racial biases.

The United Kingdom has similarly explored predictive models, particularly in assessing recidivism risk.[19] However, concerns about transparency and fairness have led to increased scrutiny and, in some cases, the suspension of certain programs.

[15]Mitchell, Machine Learning (1997).
[16]Gillespie (2014).
[17]Pasquale (2015).
[18]Angwin et al. (ProPublica, 2016).
[19]UK Ministry of Justice Reports.

China presents a markedly different model—one characterized by extensive surveillance infrastructure and integrated data systems.[20] Facial recognition, behavioral monitoring, and social credit mechanisms combine to create a highly centralized system of control.

The European Union, by contrast, has adopted a more cautious approach, emphasizing data protection and regulatory oversight through frameworks such as the General Data Protection Regulation (GDPR).[21]

These varied approaches highlight a central point: the impact of algorithmic policing is shaped not only by technology, but by the regulatory environment within which it operates.

1.5Benefits and Justification

Proponents of algorithmic policing often emphasize its potential advantages.
Efficiency is perhaps the most frequently cited benefit. By analyzing large datasets, algorithms can identify patterns that might otherwise go unnoticed, enabling more targeted allocation of resources.[22]

Consistency is another argument. Unlike human decision-makers, who may be influenced by fatigue, emotion, or implicit bias, algorithmic systems are often perceived as more stable and objective.[23]

There is also the potential for prevention. By identifying risk factors and emerging patterns, law enforcement agencies may be able to intervene before crimes occur, shifting from reactive to proactive policing.

Yet, these justifications must be weighed carefully. Efficiency, while valuable, cannot come at the expense of rights. Consistency, if built upon biased data, may simply standardize inequality.

1.6Criticism and Concerns

The criticisms of algorithmic policing are both extensive and multifaceted.

[20]Zuboff (2019).
[21]GDPR, European Union.
[22]Ferguson (2017).
[23]O'Neil (2016).

Bias remains a central concern. As discussed earlier, systems trained on historical data may replicate existing inequalities.[24]

Opacity further complicates matters. When decisions are influenced by systems that are not easily explainable, accountability becomes difficult to establish.[25]

Privacy concerns are equally significant. The data required to operate these systems is often extensive, raising questions about surveillance, consent, and data protection.[26]

Finally, there is the broader issue of legitimacy. Policing, as an exercise of state power, relies on public trust. When decisions are perceived as opaque, biased, or intrusive, that trust may erode.

1.7Conclusions

Algorithmic policing represents a profound shift in the practice of law enforcement. It introduces new capabilities—greater efficiency, predictive insight—but also new risks, particularly in relation to bias, transparency, and rights.

This chapter has sought to unpack these complexities, situating algorithmic policing within a broader global context. The next chapter turns specifically to India, examining how these technologies are being adopted and what implications they hold within the country's unique legal and social framework.

1.8 Digital Policing Initiatives in India

India's engagement with digital policing cannot be understood without reference to its broader push toward digital governance. Over the past decade, the state has invested heavily in building data infrastructures—ranging from identity systems to crime databases.[27]

One of the central pillars of this transformation is the development of integrated criminal databases. Platforms such as the Crime and Criminal Tracking Network and Systems (CCTNS) aim to digitize police records across the country, creating a centralized repository

[24]Barocas & Selbst (2016).
[25]Pasquale (2015).
[26]Solove (2008).
[27]NITI Aayog (2018).

of information.[28] This data, in turn, becomes the foundation upon which more advanced analytical tools can be built.

Similarly, the National Intelligence Grid (NATGRID) seeks to link disparate databases—travel records, financial transactions, communication logs—into a unified system accessible to security agencies.[29] While the stated objective is to enhance national security, the scale of data integration raises significant concerns about surveillance and oversight.

These initiatives, taken together, signal a shift toward data-centric policing. Information is no longer siloed; it is aggregated, analyzed, and increasingly, acted upon.

1.9 Use of Facial Recognition Technology

Among the most visible manifestations of algorithmic policing in India is the deployment of facial recognition technology (FRT). Its use has expanded rapidly, often without a clear statutory framework governing its operation.[30]

Law enforcement agencies have employed FRT in a variety of contexts—identifying missing persons, tracking suspects, and monitoring public gatherings. During large-scale events and protests, facial recognition systems have been used to scan crowds, matching images against existing databases.[31]

While such applications are often justified on grounds of efficiency and security, they raise critical concerns.

First, there is the question of accuracy. Studies conducted globally suggest that facial recognition systems may exhibit higher error rates when identifying individuals from certain demographic groups.[32] In a country as diverse as India, the implications of such inaccuracies are particularly significant.

Second, there is the issue of consent and awareness. Individuals subjected to facial recognition in public spaces are rarely informed, let alone given an opportunity to opt out.[33] The result is a form of surveillance that operates largely invisibly, yet with potentially far-reaching consequences.

[28]NCRB, CCTNS Reports.
[29]NATGRID Policy Documents.
[30]IFF, “Use of Facial Recognition in India” (2019).
[31]Media Reports on Delhi Police Surveillance.
[32]Buolamwini & Gebru (2018).
[33]Solove (2008).

1.10 Predictive Policing in Indian States

Predictive policing, though less publicly visible than facial recognition, has begun to take root in several Indian states. Initiatives in regions such as Telangana and Uttar Pradesh have explored the use of data analytics to identify crime patterns and allocate police resources more efficiently.[34]

In Telangana, for instance, law enforcement agencies have reportedly utilized predictive tools to analyze crime data and forecast potential hotspots.[35] These systems draw upon historical records, demographic indicators, and geospatial information to generate risk assessments.

While such initiatives are often framed as innovations aimed at improving efficiency, they raise familiar concerns.

The data used in these systems is not neutral. It reflects patterns of past policing, which may themselves be shaped by socio-economic and cultural biases.[36] When such data is used to predict future crime, the result may be a reinforcement of existing inequalities.

Moreover, the lack of transparency surrounding these systems makes it difficult to assess their accuracy or fairness. Details regarding their functioning, data inputs, and evaluation mechanisms are often not publicly available.

1.11 Role of Government Agencies and Databases

The expansion of algorithmic policing in India is closely linked to the growing role of government agencies in collecting and managing data. Institutions such as the National Crime Records Bureau (NCRB) play a central role in maintaining crime databases, which serve as key inputs for analytical systems.[37]

At the same time, other agencies contribute to a broader ecosystem of data collection. Aadhaar, the world's largest biometric identification system, provides a vast repository of personal information.[38] While not designed specifically for policing, its potential integration with law enforcement databases raises important questions about function creep.

[34]Telangana Police Reports.
[35]IFF Reports on Predictive Policing.
[36]Barocas & Selbst (2016).
[37]NCRB Annual Reports.
[38]UIDAI Documentation on Aadhaar.

Similarly, databases relating to telecommunications, banking, and transportation contribute to an expanding surveillance infrastructure.[39] When linked—whether formally or informally—these systems create a comprehensive profile of individuals' activities.

This aggregation of data enhances state capacity. But it also concentrates power in ways that demand careful oversight.

1.12 Lack of Transparency and Oversight

Perhaps the most striking feature of algorithmic policing in India is not its presence, but its opacity.

Information about the deployment and functioning of algorithmic systems is often limited. Official disclosures are sparse. Independent audits are rare.[40] As a result, much of what is known about these systems emerges from investigative reports, civil society interventions, and sporadic public statements.

This lack of transparency has significant implications.

Without access to information, it becomes difficult to assess whether these systems are accurate, fair, or compliant with legal standards. Accountability mechanisms—judicial, legislative, or administrative—are constrained by this informational asymmetry.

Furthermore, the absence of clear guidelines creates uncertainty within law enforcement itself. Officers may rely on algorithmic outputs without fully understanding their limitations, potentially leading to over-reliance or misuse.

1.13 Case Studies

1. Delhi Police and Facial Recognition

The use of facial recognition technology by the Delhi Police has attracted considerable attention. Reports indicate that FRT systems were deployed to identify individuals during protests, raising concerns about surveillance and the potential chilling effect on democratic participation.[41]

The lack of a clear legal framework governing such deployment further complicates matters. Without defined limits, the scope of surveillance remains uncertain.

[39]Government Data Integration Policies.
[40]Transparency Reports by Civil Society.
[41]Reports on Delhi Protests Surveillance.

2. Telangana's Predictive Policing Model

Telangana has often been cited as a pioneer in adopting predictive policing tools. Its integration of data analytics into law enforcement practices reflects a broader commitment to technological innovation.[42]

However, questions remain regarding transparency, data quality, and oversight. The absence of publicly available information about the functioning of these systems makes it difficult to evaluate their effectiveness or fairness.

3. NCRB and Data Integration

The NCRB's role in consolidating crime data highlights the centrality of information in modern policing. By digitizing records and enabling data sharing across states, it creates the foundation for more advanced analytical systems.[43]

Yet, this centralization also raises concerns about data security, privacy, and potential misuse.

1.14 Conclusion

Algorithmic policing in India does not yet present a fully formed, uniform system. Instead, it exists as a collection of practices—some experimental, others more established—gradually coalescing into a broader framework.

This evolving landscape is characterized by both potential and uncertainty. Technological tools offer new capabilities, but their deployment often outpaces the development of safeguards. Transparency remains limited. Oversight mechanisms are still emerging.

As the next chapter will explore, these developments cannot be understood in isolation from the legal framework governing data privacy in India. For it is within that framework—or its absence—that the legitimacy of algorithmic policing will ultimately be determined.

[42]Telangana Government Tech Initiatives.
[43]NCRB Data Systems Documentation.