ARTIFICIAL INTELLIGENCE IN THE CRIMINAL JUSTICE SYSTEM: A CONSTITUTIONAL ANALYSIS OF PREDICTIVE POLICING, FACIAL RECOGNITION, AND ARTICLE 21

Ms. Chhavi, Advocate

Raushan Kumar Mohan, Advocate

ABSTRACT

As one of the most promising and transformative applications of AI, it has the potential to enhance the efficiency and effectiveness of the criminal justice system, enabling law enforcement agencies to predict crime, identify suspects, monitor public areas, analyze evidence, and make decisions during investigations. Predictive policing and facial recognition are two of the most important uses of AI. Predictive policing relies on patterns of past crime and models that can predict where or who future crime may occur, and facial recognition technology is a biometric method that involves automatically matching the characteristics of a face with those in a database. The government use of these technologies brings significant constitutional issues in a democratic, rule of law society, such as efficiency, speed and crime prevention.

This paper analyses the constitutional consequences of the use of AI in police activities in India, specifically in the context of Article 21 of the Indian Constitution. The main issue that is raised is whether the practice of predictive policing and facial recognition is compatible with the right to life, personal liberty, privacy, dignity, fair procedure and protection against arbitrary acts of the State. The study is based on a doctrinal research methodology and analytical approach, using constitutional provisions, case laws, statute laws, policy documents and comparative regulatory approaches. The paper states that AI is not inherently unconstitutional in the criminal justice system, but its misuse can lead to issues like mass surveillance, algorithmic bias, misidentification, discriminatory policing, and due process violations. It finds that all the use of AI in criminal justice should meet constitutional criteria of legality, necessity, proportionality, transparency, accountability and human oversight. This is why it is important that there is a rights-based approach to legal structure so that technological innovation does not infringe on the constitutional rights guaranteed by Article 21.

Keywords: Artificial Intelligence, Criminal Justice System, Predictive Policing, Facial Recognition, Article 21, Right to Privacy, Personal Liberty, Due Process, Algorithmic Bias, Surveillance, Constitutional Law, Human Rights.

1. Introduction

AI has become one of the most impactful technological advances impacting modern governance, public administration, policing and criminal justice. Over the last few years, the criminal justice system has increasingly turned to technologies that are reliant on data for crime prevention, investigation and surveillance, suspect identification, evidence analysis, and administrative decision making. AI systems can handle vast amounts of data, detect patterns, make predictions, and help law enforcement make quicker and more informed decisions. Thus, Artificial Intelligence has moved from private commercial applications and scientific research into a tool of State power, especially in the field of policing and criminal investigations.

AI's role in criminal justice has been rationalized on the basis that it can help increase efficiency, minimize human errors, enhance crime prevention, and support complex criminality responses by the police. In traditional policing, human intelligence, witness statements, physical evidence, patrol experience and manual analysis of crime records are all key factors. AI systems can, however, analyse historical crime data, location trends, CCTV footage, biometric records, mobile data and digital evidence much more quickly. For example, predictive policing relies on algorithms and historical data to pinpoint specific areas where crimes could be committed or individuals who are more likely to be considered a threat. Likewise, facial recognition technology can be used to automatically identify individuals based on their facial characteristics captured by using camera, photographs or video footage, and a comparison against a database of faces. The use of facial recognition for identifying the criminals, missing persons, unidentified dead bodies, children has been proposed and is ongoing in India which is an example of the growing connection between policing and biometric technology.[1]

These technologies could seem as though they are helpful to public safety, but they have clear constitutional issues under the fundamental rights framework. The criminal justice system is

[1] Ministry of Home Affairs, Government of India, "Automated Facial Recognition System will facilitate better identification of criminals, unidentified dead bodies and missing/found children and persons," Press Information Bureau, 4 March 2020.

not just another administrative matter, it impacts on the life, liberty, dignity, reputation, and body autonomy of people. This can lead to greater surveillance, arbitrary questioning, arrest, custodial harshness or social stigma if the algorithmic prediction, facial match or the dataset is inaccurate, or the technological decision is opaque. The constitutional issue is not just about whether AI can improve the efficiency of policing – it is whether this efficiency can be maximised without doing so. Science and technology cannot replace legality, fairness, accountability and due process in a constitutional democracy based on the rule of law.The Supreme Court in a series of landmark cases has extended the ambit of Article 21 of the Constitution of India, which protects the right to life and personal liberty and states that the right to life and personal liberty will not be taken away from any person unless procedure established by law is followed.[2] In Maneka Gandhi vs. Union of India, the Supreme Court explained that the procedure envisioned by the Article 21 shall be fair, just and reasonable and must not be arbitrary, fanciful, or oppressive in nature.[3]This interpretation shifted Article 21 from a limited right against the deprivation of liberty to a constitutional safeguard against arbitrary state action. Thus, any AI policing system pertaining to personal freedom shall be considered constitutional if it is deemed to meet the requirements of fairness and reasonableness.

The right to privacy adds to the constitutional challenges of AI in criminal justice. The landmark Justice K.S. Puttaswamy v. Union of India decision highlighted that privacy is an integral part of Article 21, the right to life and personal liberty, and any infringement on privacy must meet the test of legality, legitimate State aim, necessity, and proportionality, all of which are applicable to facial recognition and predictive policing.[4] In particular, facial recognition is particularly sensitive, as the human face represents a permanent biometric identifier and cannot be altered like a password, identification number etc. With facial data captured and matched to State databases, people can be identified and tracked in public areas without their awareness and permission.[5]

This concern is reinforced by the Supreme Court's ruling in Anuradha Bhasin v. Union of India, which held that any State restriction on rights, including one justified on security grounds, must

[2] The Constitution of India, art. 21.
[3] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[4] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[5] Ibid.

satisfy the test of proportionality and cannot rest on unreviewable, unpublished justification.[6] The same logic applies with equal force to AI-enabled mass surveillance and facial recognition, which risk producing an unchecked chilling effect on the exercise of civil liberties in public spaces.

The other constitutional issue is that predictive policing can introduce a new form of suspicion: algorithmic.Predictive policing introduces yet another serious constitutional quandary: algorithmic suspicion. An individual can be stopped by the police without any specific criminal offense, since the algorithm determined that a locality or a community or a behaviour is dangerous. The algorithm can perpetuate and amplify historical policing bias if the data it relies on is itself historically biased. This can result in the over-policing of specific communities, neighbourhoods and socio-economic groups. The use of AI in policing needs to be analysed through the lens of equality, liberty, dignity, privacy and fair procedure, not only in regard to Article 21 but also Article 14 prohibiting arbitrary and discriminatory State action.[7]

The research problem that has been raised in this paper is whether use of Artificial Intelligence in the criminal justice system, in particular predictive policing and facial recognition technology, can be constitutionally justified under Article 21? It explores the need for a dedicated rights-based regime for AI-driven policing, questioning whether current laws are adequate to safeguard against algorithmic bias, mass surveillance, misidentification and accountability issues. This paper aims to examine the constitutional dynamics of AI tools in the criminal justice system and question what protection is needed to ensure their use is legitimate and equitable.

This paper uses doctrinal and analytical research methods. Examines the relationship between AI and constitutional rights using constitutional provisions, judicial precedent, statutory resources, government policy documents and comparative regulatory strategies. This paper seeks to analyse the constitutional dimensions of predictive policing and facial recognition in the criminal justice system, focusing on Article 21 of the Constitution. Wherever possible, however, references to articles 14, 19 and 20(3) are included as constitutional rights frequently intertwine. The paper does not state that the use of artificial intelligence in the criminal justice system is inherently unconstitutional; however, its misuse in criminal justice in an increasingly

[6] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
[7] The Constitution of India, art. 14.

disproportionate, opaque, and unregulated way can turn it into a constitutionally problematic practice. Thus, the direction of AI in policing should be not just technologically efficient, but also aligned with constitutional morality, the rule of law, the dignity of persons and the protection of personal liberty.

2. Artificial Intelligence in Criminal Justice: Meaning, Scope and Emerging Uses

AI in the Criminal Justice System is the application of computer systems that can analyze data, detect patterns, make forecasts, identify objects or persons, categorize information, and support human decision-making. AI systems can tell police, investigators, and other law enforcement agencies how to respond to crime, analyze the data at their disposal and output results that can help them with investigations, help prison staff manage inmates, and impact how judges rule. These AI systems are not just more efficient at recording digital data; they can analyze the data available to police and other law enforcement agencies and produce results and outputs that will affect how police and investigators should respond to crime, how prison staff should manage inmates, and how judges make decisions. AI is used in criminal justice in various areas, such as machine learning, data analysis, natural language processing, computer vision, biometric identification, and automated risk assessment. The significance is that a tremendous amount of data is generated and processed by criminal justice institutions, such as FIRs, charge-sheets, arrest records, CCTV footage, call detail records, forensic reports, prison records, court records, and criminal databases. AI is thus offered as a means to organise this information and help the State in crime control and public safety.

AI's potential applications in criminal justice are extensive, as it can be applied in nearly all stages of the criminal process. AI can help in policing by crime mapping, deployment of cops, crime identification, monitoring public areas, and analyzing past crimes. It can be utilized during investigation for suspect identification, facial recognition, digital forensics, cybercrime analysis, document classification, voice identification and reconstruction of events in electronic records. During the prosecution and court process, AI can assist in case management, legal research, document review, and e-evidence analysis. Digital systems can contribute to prisoner management, visitor management, monitoring parolees, risk assessment and connecting prison information with police and court records at the prison stage. AI is not one technology but a collection of tools which can have an impact on the criminal justice continuum. One of the most talked about applications of AI in the criminal justice system is predictive

policing. It involves predicting the probability of crime on the basis of historical data on crime, geographical data, police data, time patterns and other factors. Predictive policing can take a location-based approach, by predicting locations that are likely to have criminal activity, or a person-based approach, by predicting who is likely to be a criminal or victim of a crime based on previous data. Administratively, these can be used by police departments to make resource allocation decisions, to plan for certain areas, and to react swiftly to a new trend in crime. It is conceptually sensitive, however, in its turn from the reactive model of policing to a preventive and anticipatory one, as it is done under predictive policing. The police are not just reacting to crimes reported to them – the police can take action in anticipation of potential crime, based on algorithms. This renders the concept of 'predictive policing' very relevant to the analysis of the Constitution, particularly if the prediction has an impact on liberty, movement, reputation or police treatment of specific communities.[8]

Another significant AI application in the criminal justice sector is facial recognition.[9] It works by transforming a human face into a template of human identifiers and trying to match it with a template stored on a hard drive or in a database. Facial recognition can be used for finding a suspect in a video captured by a CCTV camera, to find a missing person, to identify a body without a known identity, to track an accused absconding suspect, or for surveillance at public events. Facial recognition thus in India is a direct link between biometric technology and policing, with the Government calling the technology an instrumentation to help identify criminals, unidentified dead bodies, missing persons and children.[10] But, since the human face is a lasting, public identifier, facial recognition also poses risks of mass surveillance, constant tracking, misidentification and unconsensual data processing.

The presence of crime maps and CCTV surveillance systems also show the increasing technological nature of policing. Crime mapping is the process of visually and statistically analyzing crime incidents by location, time, crime type, modus operandi, and crime recurrence. AI-powered crime mapping can assist with spotting crime hotspots, patterns, and potential crime-facilitating connections when combined with data analysis. The implementation of

[8] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 18–24 (New York University Press, 2017).
[9] NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology 13–18 (Government of India, 2022).
[10] Ministry of Home Affairs, Government of India, "Automated Facial Recognition System will facilitate better identification of criminals, unidentified dead bodies and missing/found children and persons," Press Information Bureau, 4 March 2020.

CCTV is a great way to monitor public spaces in real time, especially when combined with video analytics and facial recognition. Modern surveillance systems can identify unusual movement, unattended objects, crowds, vehicle registration numbers and/or individuals on watchlists. The tools can be useful in an emergency response and investigation but can also produce an ongoing environment of data that allows for the collection, analysis and recording of normal public travel by the State.

Another significant field where AI is becoming increasingly applicable is digital evidence analysis. Digital evidence analysis is also a crucial field where AI is gaining relevance. Mobile phones, computers, CCTV footage, social media, financial records, GPS data, emails, call records, cloud storage and encrypted communication are all part of the tools that are used in contemporary criminal investigations. It may be difficult and time consuming to analyze this data manually. AI-powered tools can help investigators organize documents, find keywords, recognize patterns, connect digital transactions, analyse images or videos, and monitor online activity. The crime and criminal tracking network and systems were developed to enhance efficiency and effectiveness of policing by establishing an integrated digital system at the police station level, whereas the digital police portal was created so that investigators have access to criminal records and analytical search function.[11] These features show the trend of transitioning from fragmented police records to a unified data-driven investigation.

Another area that's new to AI in criminal justice is risk assessment. Algorithmic instruments are employed in some jurisdictions for predicting a reoffending risk, the risk of absconding, threat level, or the suitability for bail, parole and probation, or sentencing-related decisions. While India has not followed such models like certain foreign jurisdictions, the idea that such tools might be implemented in the future is significant. The use of risk assessment tools generates concerns that could affect decisions that impact upon personal liberty. Tools that are based on incomplete, biased, or opaque data can lead to imbalanced results. Thus, the concept of a risk assessment should not be interpreted only as an administrative tool, but as a technology that can have an impact on constitutional rights in the context of arrest, release, parole and classification of custody.

[11] Ministry of Home Affairs, Government of India, "New Features/Uses for Police Investigation in CCTNS/ICJS," 12 April 2023; Ministry of Home Affairs, Government of India, "CCTNS Digital Police Portal Launched to Fast-track Criminal Justice Delivery," Press Information Bureau, 6 October 2017.

AI and digital governance are also seen in the administration of prisons. Prison management systems can be used to keep records on prisoners, track the admission and departure of inmates, control visitors, store parole data, process legal assistance and tie prison data with judicial and police departments.[12] These modules could enhance the effectiveness of criminal justice administration and coordination among criminal justice agencies in India. But, as prison data is joined with police and court data, issues of data accuracy, access and privacy and misuse become important.

One of the most widespread applications of AI is in the field of investigation support. AI could help investigators by reading and connecting FIRs, identify repeat offenders, analysing modus operandi, matching forensic evidence, summarising case material, preparing investigation leads, and inconsistencies in records. This illustrates that the future of criminal justice is to integrate data from police, prisons, forensics, prosecution and courts, and also run investigations with the help of data analytics and AI/ML tools.[13] However, it's crucial that AI is not a decision-maker but a tool to assist in making decisions. In criminal justice, any technological output should always be considered an investigative lead, one that needs to be investigated, verified, lawfully reviewed and properly protected. The promise and potential of AI in criminal justice are therefore both promising and problematic; it can aid in efficiency, but it can also escalate surveillance, bias, and arbitrary governmental power, if it is not regulated.

3. Article 21 and the Constitutional Limits on AI-Based Policing

The meaning of Article 21 has been interpreted by the courts as one of the strongest protection from arbitrary action by the State and despite the apparent simplicity of the text the Article has been interpreted with great breadth. With respect to the meaning of "life and personal liberty" in the Constitution, the Supreme Court has held that it is not only protection against physical restraint, or the deprivation of life, but also a wide-ranging constitutional right to dignity, privacy, autonomy, bodily integrity, fair procedure, access to justice, or protection from unlawful interference by the State. This wider interpretation of Article 21 takes on new meaning in the environment of policing delivered by Artificial Intelligence (AI) technology, as

[12] National Informatics Centre, Government of India, "e-Prisons"; e-Committee, Supreme Court of India, "e-Prisons," 28 August 2020.
[13] Ministry of Home Affairs, Government of India, "Inter-Operable Criminal Justice System," 13 September 2024.

it is the intersection between State power and individual freedoms.[14]

The significance of Article 21 in the constitution is that criminal justice is the field in which the coercive power of the State is most apparent. Activities of policing, surveillance, arrest, search, interrogation, investigation, detention, prosecution are all acts that will directly infringe one's personal liberty. Thus, no technological solution in the field of criminal justice can be assessed just on the criterion of administrative efficiency but also on the constitutional control criterion. Predictive policing, suspect identification, evidence analysis, and public surveillance are some areas where AI-driven policing can help law enforcement agencies. If they are not accompanied by legal protections, however, they can lead to arbitrary surveillance, mistaken identification, discrimination against targeted individuals and inaction and deprivation of liberty without fair procedure. Article 21 thus serves as a constitutional fence to protect against the misuse of AI by police.

In Maneka Gandhi v Union of India, the Supreme Court did not accept a narrow reading of Article 21 and concluded that the process that led to the deprivation of life or personal liberty has to be "right, just and fair" and not arbitrary, fanciful or oppressive" and that the deprivation could only take place after the procedure is found to be so.[15] This is the same in the context of policing with AI. The use of an algorithmic alert or facial recognition match in a process leading to an arrest, detention, or surveillance of a person must be fair, reasonable and legally accountable. No secret or unclear algorithm can be a replacement for constitutionally valid procedure.

The case of Maneka Gandhi is relevant because AI-driven policing frequently works via technology that is not comprehensible to the general public, police, lawyers or even courts. Predictive policing models can be based on historical crime data, arrest records, demographic information, location information, or behavioral information. Facial recognition systems can provide matches by using biometric templates in comparison with existing databases. The person concerned, however, may be unaware of the information that has been used, how the system came to its conclusion, what error rate there is and whether the system has been audited independently. This lack of clarity is a serious due process issue. The state action under Article 21 must be justifiable. In the field of criminal justice, AI systems must be explainable and

[14] The Constitution of India, art. 21.
[15] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

reviewable and open to human oversight.

In Puttaswamy, the Supreme Court observed that privacy is a fundamental aspect of life, personal liberty, dignity, and autonomy under Article 21 and that there are four types of privacy viz, bodily privacy, informational privacy, decisional autonomy and control over personal data.[16] The principle is important for the technology of predictive policing and facial recognition as they both rely on the collection, storage, processing and analysis of personal data. Biometric data is much more sensitive than any other type of data, especially the face, which is a permanent representation of identity. Location, criminal history, social connections, neighbourhood data and behavioural information are all examples of data that could be used for predictive policing. The use of data directly relates to the constitutional right to privacy.

Puttaswamy also laid down the constitutional check on State action that infringes upon the right to privacy. For the purposes of AI-based policing, this requirement translates to the necessity for having a legal basis, pursuing a legitimate State aim and satisfying the requirement of proportionality for the use of facial recognition and/or predictive policing. There should be clear legal accountability for why it exists, how it is used, its boundaries, a supervisory mechanism, retention policy, and sanctions for misuse. Surely the State can use the arguments of crime prevention and public safety as legitimate goals, but legitimacy of aim is not enough. The approach taken should also be necessary and proportionate. Where there are no less intrusive methods, mass biometric surveillance or continuous algorithmic tracking might not meet the proportionality test.[17]

This procedural requirement is not a novel one. Long before Puttaswamy, in People's Union for Civil Liberties v. Union of India, the Supreme Court dealt with unregulated telephone tapping by the State and held that surveillance without procedural safeguards infringes Article 21, directing that interception be authorised only by a designated senior authority, for a limited duration, and subject to periodic review.[18] The same principle of authorisation, purpose-limitation and periodic review that the Court read into telephone surveillance applies with equal, if not greater, force to AI-based predictive policing and facial recognition, which are capable of monitoring far larger numbers of people with far less individualised justification

[16] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[17] Ibid.
[18] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

than telephone tapping ever required.

Violation of the principle of proportionality is particularly relevant as AI-powered policing could impact on many individuals who are not facing any charge. Traditional criminal investigation typically occurs as a result of a complaint, suspicion, evidence or recognisable offence, all of which are conducted by the State.Traditional criminal investigation involves State action, which generally follows a complaint, suspicion, evidence or identifiable offence. But predictive policing and facial recognition could be preventive, and generalised. Whole neighbourhoods can be deemed high risk and common folk can be monitored as they wander through public spaces. These practices can normalize suspicion, and can turn public spaces into places of constant State surveillance. Article 21 does not allow the State to suspect a person to be a suspect if there is no law, necessity, and proportional safeguards.[19]

The Supreme Court's judgment in Selvi v. State of Karnataka[20] is also relevant for assessing the constitutionality of scientific tools like the narco-analysis test, the polygraph test and brain mapping in a criminal investigation. In addition, the Court ruled that investigative procedures cannot be justified simply because they may aid in the detection of crime. The Selvi logic is equally applicable to the investigation with the help of AI, as it is clear that technology does not cancel out constitutional rights. Any technique can be useful scientifically but must be within constitutional bounds.

The principle gleaned from Selvi is that the person is not just the source of information for the State for the criminal process. The worry with AI-based policing is similar. The status of an individual as a rights-bearing person can be diminished when they are treated as a data point, biometric template, risk score or algorithmic category. A person can be deemed risky without any individualised evidence, as predictive policing can be used to label individuals as risky. Facial recognition might be used to identify someone as the result of automated matching without any meaningful consent or chance to dispute the indicated match. This may involve a consideration of dignity and autonomy as enshrined in Article 21. Thus, the use of AI tools should be used in an assistive capacity and must not replace or be a substitute for legally defined concepts like reasonable suspicion, probable cause, corroborative evidence, and judicial

[19] Ibid.
[20] Selvi v. State of Karnataka, (2010) 7 SCC 263.

review.[21]

D.K. Basu v State of West Bengal is another example of the use of Article 21 to manage police power, in which the Supreme Court provided guidelines to curb the use of violence, arbitrary arrests and misuse of power by police. The judgment acknowledges that arrest and detention have a direct impact in violation of the dignity of the person and the right to personal liberty, and therefore, the need for procedural safeguards. Relevance of D.K Basu to AI based policing is more broadly based principle of police powers being subject to accountability, transparency and enforceable safeguards. Where there is a legitimate need for protection of the procedural rights of an individual subject to traditional arrest and detention, the same is equally true of a group of individuals subject to AI-generated suspicion and police action.[22]

Another issue is accountability with AI-driven policing.There's also the issue of accountability in AI policing. A false match by a facial recognition system or a misidentification in a predictive policing system can be hard to determine who's at fault. The police could say it was the software, the software company could say it was the data and the government department could say it was the technical limitations. This type of diffusion is unconstitutional when personal freedom is involved. Article 21 stipulates that each restriction on liberty be traceable to a lawful authority and be open to challenge. Thus, any AI system employed in criminal justice should have audit trails, human decision makers, documentation of reasoning, and correction and compensation processes.

In light of the constitutional restrictions imposed by Article 21, it is necessary to take a rights-based approach to criminal justice and AI. First, it's legal and has explicit statutory powers to use AI in policing tools.First, the use of AI tools in policing has to be legal with clear statutory powers. Secondly, there should be necessity, that is, the tools should only be used if they are actually needed for a legitimate criminal justice purpose. Thirdly, there has to be proportionality, that is the harm done to privacy and liberty cannot override the public good that is gained. Fourthly, transparency and explainability must be achieved, allowing those who are impacted and courts to understand and review the ground for action provided by AI. Fifthly, there needs to be procedural fairness, such as human oversight, independent audits, data protection measures and remedies in the event of misuse.

[21] Ibid.
[22] D.K. Basu v. State of West Bengal, (1997) 1 SCC 416.

Therefore, there is no restriction in Article 21 on using Artificial Intelligence in criminal justice. It does not allow for the arbitrary, opaque, disproportionate and unaccountable use of AI. The Constitution is not opposed to technological innovation, but only to technological innovation that is subordinated to liberty, dignity and privacy, as also to rule of law. AI can be used by policing but cannot be a substitute for constitutional judgment. It can be a source for investigation but it will not be enough on its own for arrest, detention or criminal liability. The final constitutional stance is that any AI application that is utilized in criminal justice sector should meet the threshold of legality, necessity, proportionality, transparency, accountability and fair procedure. Violation of these safeguards could potentially infringe on the spirit of Article 21 in the case of the use of AI in policing.

4. Predictive Policing and the Problem of Algorithmic Suspicion

Predictive policing is a particularly controversial use of AI in the justice system, which tries to predict crimes that will happen before they happen. Typically, it applies data analytics, statistical modelling, machine learning and algorithmic tools to forecast "hot spots," potential criminals, vulnerable victims or criminal activity. Predictive policing is not about responding to reported crimes or suspicions as is traditional policing, but about probability. This has made predictive policing appealing to police as it will help them to be efficient, respond quickly and provide prevention-based policing.

There are in general two types of predictive policing. The first one is place-based predictive policing which is used to target geographical areas, or “hotspots,” where crimes are more likely to be committed. Such systems are based on previous crime information, FIR information, emergency calls, location, crime time, and repeat crime information. The second is “person-based predictive policing,” which tries to find people who might be more likely to commit crimes or be crime victims. Person based systems can be based on past convictions, social groups, police intelligence, demographic data, behaviour or on previous interaction with law enforcement agencies. Place-based systems are not as intrusive as person-based systems, but each can impact constitutional rights when the results impact the process of surveillance, patrolling, questioning, detention or arrest.[23]

The fundamental conceptual challenge of predictive policing is that it could lead to what can

[23] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement 18–24 (New York University Press, 2017).

be termed "algorithmic suspicion." For ordinary criminal law, suspicion is required to be founded on facts of the person, acts, evidence, complaint, or circumstances, which establish the identity of the person with an act or a violation of the law. Predictive policing reverses this pattern, so that suspicion can be generated based on a statistical classification. It may be possible for a person to be treated as suspicious even though none of the criteria apply to any specific crime, but rather because they reside in a certain area, are connected to a certain network, have a history of police contact, or fall into a certain data pattern identified by the algorithm. This is constitutionally dangerous as criminal justice in a liberal constitutional system is predicated on individual responsibility, and not collective or statistical suspicion. Article 21 specifies that state action that impinges on personal liberty must be fair, just and reasonable; that is, it is not sufficient that the algorithm is suspected of infringing on personal liberty; there must be individualised reasons for it.[24]

This makes the situation worse since predictive policing relies heavily on police data. This information is not necessarily unbiased or factual. Recorded crime is not necessarily the same as actual crime and includes only those crimes that are reported to, and recorded by, police agencies, and then investigated and given a priority. More arrests or complaints could be made from areas of the neighbourhood that historically have seen more police presence. A computer program designed with information like this can then pinpoint the same places as being at high risk, which may then cause more police presence in those areas. The more the algorithm is used, the more recorded incidents it will generate, further reinforcing the algorithm's conviction that an area is crime prone. This establishes a vicious circle in which the actions of police in the past become the policies for future police action.[25]

This has become a vicious circle and poses concerns under both Articles 14 and 21. Article 14 guarantees the right against arbitrary and discriminatory action by the State, and Article 21 guarantees liberty, dignity, privacy and fair procedure. Predictive policing may have a disproportionate impact on poor neighbourhoods, different racial and ethnic communities, migrants, informal workers and socially marginalised groups if the historical policing data already shows an imbalance in policing. Under those circumstances, the algorithm doesn't eliminate human bias: it might conceal it and repeat it behind the guise of the neutral

[24] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[25] Rashida Richardson, Jason M. Schultz and Vincent M. Southerland, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice" 94 New York University Law Review Online 192 (2019).

technology. This is one of the greatest risks of using AI in criminal justice: If a human justice officer makes an unfair decision, it can be argued that it's a matter of discrimination, but an algorithm can seem scientific, objective and data-driven.

It is especially crucial in India where policing historically has featured broad discretion, preventive powers, local intelligence systems and social profiling. The potential danger with this kind of policing in combination with AI systems is that the informal suspicion can become formal data and then automated prediction. For instance, if data in the police's databases is duplicated across various communities or localities as a result of previous surveillance, this algorithm could consider such communities to be inherently dangerous. This can lead to more police officers being deployed, questioning more people, conducting more stop and search operations and more surveillance. These practices can be a breach of the dignity of a person, by suspecting them permanently. Article 21 does not allow the State to classify people in terms of risk scores or data categories without proper legal reason and protection.Predictive policing also poses an issue to the presumption of innocence. In general, the principle of the criminal law is that a person is presumed to be innocent until they are shown to be guilty. Predictive policing is not an imputation of guilt, but it could inform police actions in a way that diminishes this. A risk person might be supervised, intercepted, questioned or suspected before they have committed any crime. A shift from evidence-based investigation to risk-based surveillance is altering the moral landscape of criminal justice. It is not because the person has committed a law violation, it is because the system expects, or forecasts, that a law violation will occur. Such a preventive logic needs to be tightly monitored or it can become part of a normalised culture of surveillance and suspicion.

The other significant issue is opacity. Most predictive policing models are not easily decipherable by police, accused, lawyer or the courts. When an AI system flags a specific information source or a specific person as being high risk, it may not be known what data has been used, how it has been weighted, what assumptions the model is based on, or if it has been independently audited. This presents a due process dilemma. The individual has to have a meaningful mechanism for challenging the underlying basis of the State action if they are afflicted by AI supported policing. Once the algorithm is used as a black box, it's hard to determine if the prediction proved to be correct, inaccurate, biased, misdated, or if it was made on illegal data. In the context of Article 21, the issue of fair procedure implies that any act of infringement on liberty must have grounds that are public, at least challenging and not secret.

There are accountability issues with predictive policing as well. When police officers rely on an algorithmic prediction, and that prediction leads to an unjustified arrest, harassment, or discrimination, it's hard to identify who is at fault. Police might have said they used a technological tool and the software company might said that the software just gave a probability, not a directive on how to act. This diffusion of responsibility is very harmful in the criminal justice context because liberty depends upon clearly assignable responsibility. Article 21 requires that all interference with personal liberty be legally justified and can only be attributed to responsible State action. This means that police officers cannot be held accountable for the consequences of their actions while relying on AI tools to justify any wrongdoing as an "error" or "mistake".

India also has crime mapping and predictive systems that indicate a shift towards data-driven decision making in policing. Administratively speaking, crime mapping and analysis systems with real-time and historical data can be used to determine crime hotspots and help inform deployment decisions, particularly in large urban areas with limited police resources and crime patterns that are complex. But their constitutional validity will rely on the protection afforded to their use. A system to help allocate resources internally could be less intrusive than a system for arrest, targeting, and/or surveillance. The more that a law impinges upon liberty and privacy, the more its constitutional limits will be examined.[26]

Predictive policing is not a problem that should simply be ignored, rather it should be controlled with robust safeguards. First, predictive policing goes to need legal support. It should not just function by executive order, pilot initiatives or technological solutions driven by vendors. Secondly, there should be a clear definition of the purpose of the system. It should only be used to prevent and investigate crime and not for the purposes of general social control. Thirdly, the data should be accurate, relevant, updated and unbiased (no discriminatory elements). Fourthly, independent bias audits and regular review of the system. Fifthly, the predictions of algorithms should not be a reason in their own right for arrest, detention, search, or police coercion. Their use should only be a way of deriving investigative leads that need human verification and corroborative evidence.

Above all, predictive policing should meet the criteria outlined in Article 21 of legality, necessity, proportionality, transparency and fair procedure. There must be a law to justify actions as legal. There should be a genuine need for the tool in relation to a policing need.

[26] Vidhi Centre for Legal Policy, "India's Tryst with Predictive Policing," 13 April 2020.

Proportionality must mean that the infringement of privacy, dignity and liberty must not be disproportionate to the public benefit that is gained. To be transparent, the system should be provided with meaningful disclosure about what the system is, how it is used, and its limitations. Fair procedure needs to be backed by human oversight, reasons for action, auditability and remedies for wrongful use. If not these protections, predictive policing can turn the criminal justice system into an automated suspicion machine.

Predictive policing is therefore a boon and a bane. It can help police to detect crime patterns and better utilise resources. Without constitutional protections, however, it can perpetuate history and worsen over-policing, undermine presumption of innocence, and endanger personal liberty. The problem is not that prediction is never allowed, but that algorithmic prediction cannot be a substitute for individualized suspicion, evidence and due process. In a constitutional democracy, policing has to be held to account by law and not just facts and figures. Hence, predictive policing should be used as limited investigative tool and not as a grounds for State coercion.

5. Facial Recognition, Privacy and Mass Surveillance

One of the most sensitive applications of Artificial Intelligence in the criminal justice system is facial recognition technology, as it directly links biometric identity to the State surveillance. The way it works is to detect a human face, measure the face's features, encode them into a biometric template, and find a match for it in an existing database of images. Police use facial recognition for detecting suspects in CCTV footage, to locate missing people, to find unidentified dead bodies, to track crowds at public events, or to look for people in criminal databases. The law enforcement perspective is that this technology could be beneficial in helping investigations when traditional evidence is scant or when a suspect cannot be identified in a video of an incident.

The application of facial recognition in police work in India has been justified primarily for crime prevention, identification of criminals, missing persons and unidentified bodies. The constitutional issue does not just stem from the purpose of the technology being brought in, the Ministry of Home Affairs has said though police records would be used in the Automated Facial Recognition System.[27] Even if the object is legal, the method used in achieving it should

[27] Ministry of Home Affairs, Government of India, "Automated Facial Recognition System will facilitate better identification of criminals, unidentified dead bodies and missing/found children and persons," Press Information Bureau, 4 March 2020.

meet constitutional requirements. The same technology used to identify people in public areas can be used to track, profile and perpetuate surveillance. In this context, the issue of facial recognition needs to be discussed in the context of privacy, dignity, liberty, autonomy, and procedural fairness as provided in Article 21.

The greatest concern with the constitution is the right to privacy, which is being affected by facial recognition. The Supreme Court in Justice K.S. Puttaswamy v. Union of India has acknowledged privacy as an integral part of Article 21 of the Constitution of India, encompassing informational privacy, bodily privacy, decisional autonomy and control over personal data.[28] All these dimensions are impacted by facial recognition. The face is not just a physical part of a person, it is a permanent biometric identifier that is associated with identity, movement, association and presence in public space. A face can't be easily changed like a password or an ID number. Facial data collected, stored and correlated with State databases can be reused multiple times for identification and tracking without meaningful knowledge and consent of the individual.

Mass surveillance is also a problem of facial recognition. Traditional state surveillance typically demands that there be some specific reason, for example investigation of a specific offence or monitoring of a specific suspect. The use of facial recognition, particularly in relation to CCTV networks and public databases, can be used to provide generalised scanning of large populations. People can be recorded and matched with databases without the need to suspect any one person when they are moving about in a railway station, a market, a protest, in court, in an airport, or in a public road. It alters the attitude of the citizen towards the State. Public mobility becomes a source of biometric information and anonymity in the public sphere is limited. Such a system could lead to a society in which anyone can be known, monitored and tracked at all times.

This is an important concern, especially because Article 21 guarantees not only physical freedom, but dignity and autonomy. Individuals should not be subjected to continual suspicion in order to satisfy human dignity. If widespread and unprotected, facial recognition could have a chilling effect on normal democratic processes. If citizens are fearful that they might be recorded and identified by the State, they may avoid protests, political gatherings, religious services, social issues campaigns, and other sensitive public events.Citizens might be afraid to

[28] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

attend protests, political meetings, religious services, social issue campaigns, or other public events with sensitive social issues. While mainly focused on Article 21, this chilling effect is also related to the Article 19 freedoms of speech, association, assembly and movement.[29] The same rationale could be applied to the case of biometric surveillance, where the potential for being monitored de-incentivises consent to participate in public life. The Supreme Court's reasoning in Anuradha Bhasin v. Union of India lends further support to this concern, as the Court held that restrictive State measures affecting the exercise of fundamental freedoms must be the least intrusive option available and cannot be open-ended or indefinite; the same proportionality-based scrutiny applies to mass biometric surveillance through facial recognition, which by its very design operates as a continuous and generalised, rather than a targeted and time-bound, measure.[30]

The other big worry is the possibility for wrongful identification. Facial recognition systems don't yield absolute truth, they generate probabilistic matches. A false positive is when a suspect is falsely identified as a non-suspect. A criminal justice error could have a serious impact, such as police questioning, detention, arrest, damage to reputation, custodial harassment, and the length of the litigation. The risk of the constitution is therefore much greater than for regular administrative use of technology. Where a match is incorrect in a commercial setting, there may or may not be a loss of inconvenience; however, an incorrect match in the policing context may lead to deprivation of liberty. Article 21 mandates that every decision that involves liberty shall have to be taken through a fair, reliable and legally accountable procedure. Hence, a facial recognition "match" should not be considered conclusive evidence or a standalone basis for arrest.

The concern with due process is heightened by the opacity of facial recognition systems. The impacted person might not even be aware of face recognition, database accessed, accuracy rate of the system, whether images were good enough or whether the system was biased, or whether a human officer verified the outcome. This puts a huge imbalance in proceedings. Lack of disclosure of the basis of the technological match means that the accused has no meaningful opportunity to challenge the evidence and/or investigation. Article 21 of the Constitution guarantees that criminal justice decisions should be open to challenge on the basis of the principle of 'fair procedure'. There should be no secret biometric matching to underpin State

[29] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[30] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

action.

Another challenge with facial recognition is bias and discrimination. AI systems are developed using data sets, and the quality of the data sets determines the accuracy of the AI system. An imbalanced system that performs poorly for one group due to their age, gender, skin tone, picture quality, socio-economic status, etc., can lead to disproportionate identification or monitoring. This technological bias can exacerbate social disparities already present in India's access-to-justice framework and policing outcomes. This concern relates to both Articles 21 and 14, as it is not acceptable technologically to be arbitrary or discriminatory, even if it is automated.

But there's no dedicated law concerning facial recognition in criminal justice, which makes this problem more serious. India has no specific legislation on facial recognition by law enforcement authorities at the moment, which sets out in detail on whom the police may search, what level of suspicion they must have, how long the biometric data can be kept for, to whom it can be accessed by, whether independent approval is required, and what the remedies are if the data is wrongfully identified. The principle of general data protection does not sufficiently serve the purpose of criminal justice use of biometric surveillance, as it has a direct impact on liberty that demands a more specific safeguard.[31]

In the light of the requirement in Puttaswamy for constitutional legality, legitimate aim, necessity and proportionality, the constitutional validity of the use of facial recognition in criminal justice seems to be possible only when the use is authorised by law, for a clearly defined serious purpose, it is necessary for that purpose and it is proportionate to the rights affected. The State shall also have to prove that there is no practicable less intrusive alternative. For instance, it might be easier to justify targeted use of facial recognition in a particular investigation than on a real-time basis of all people in a public place. As the technology grows in scale, intrusiveness and impact, the constitutional review and analysis should become more robust.[32]Facial recognition should not be used as an everyday policing tool but one that has a high risk associated with it. It should be subject to comprehensive protections, including statutory authorization, purpose limitation, prior independent risk assessment for high-risk applications, data minimisation, temporally limited retention, accuracy testing, bias audits,

[31] The Digital Personal Data Protection Act, 2023.
[32] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

human verification, audit logs, transparency reports and remedies for misidentification. Most importantly, a facial recognition match should only be used as an investigative lead when it is backed up by further and admissible evidence. The use of facial recognition is not prohibited by Article 21, but it is prohibited when used in an arbitrary, secretive, disproportionate and unaccountable way. Biometric technology in a constitutional democracy should be subject to the principles of privacy, dignity, liberty and due process.

6. Evidentiary, Procedural and Accountability Concerns

What constitutes evidence for the AI-generated evidence is a critical question in criminal justice that requires consideration.There is an important question regarding whether the AI-generated evidence is considered evidence or if it is just an investigative lead in criminal justice. Predictive policing alerts, facial recognition matches, algorithmic risk scores, automated CCTV analysis and digital pattern recognition can help police find and stop criminals, but should not be automatically assumed to be evidence of guilt or grounds for coercive action. Criminal law is based on evidence that is legally admissible, reliable and is tested. Results provided by AI typically have probabilistic elements and rely on the quality of data, the accuracy of the algorithm, the clarity of the images, training models, the integrity of the database and the human interpretation. Thus, the outputs should be used with caution in the criminal process.[33]

For example, if a person's face is matched in the database, this does not automatically mean that they have committed an offence. It simply tells if there is any similarity between two images in the database. Likewise, a predictive policing alert isn't a prediction of a crime or of who is likely to commit a crime. It only gives a statistical forecast on the basis of the available data. If this type of output is considered to be adequate base for arrest, detention, interrogation, or prosecution, the criminal justice system could shift from evidence-based investigation to algorithmic suspicion. This would not be consistent with Article 21 which provides for a fair, just and reasonable procedure before deprivation of liberty.[34]

The first big procedural issue is that of the algorithms being black boxes. A lot of AI systems are based on complicated mathematics that is not easily understandable for non-technical users.

[33] NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology 21–28 (Government of India, 2022).
[34] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.

The output of such tools may not be understood by even the person using them, even police officers. This opacity is problematic in criminal matters as the accused needs to contest the grounds of State action. When relying on a face match or the inference or application of AI, the defence should have a meaningful opportunity to review the data, method, error rate, and reliability of the system. The lack of explanation or testing of a technological result ought not to permit it to be the basis of criminal responsibility. Transparency is an element of a fair trial and contestability is an element of a fair trial.

The second concern is with electronic evidence and chain of custody issues. The outputs of AI are typically based on electronic records like CCTV footage, digital images, call logs, social media data, device data, GPS logs, or database records. The material should be collected and preserved in a legally sound way, transferred, stored and produced in front of the court. A lapse in chain of custody can raise suspicion that the sample is not genuine, has been tampered with, manipulated or substituted. The Supreme Court pointed out that electronic evidence "must meet the statutory requirements for adducing the evidence and, in the case of secondary electronic evidence, that the secondary evidence is produced before the court".[35]

The principles set forth in Anvar are highly applicable to the tools used in criminal justice that involve AI. When a match is obtained from the CCTV footage, the prosecution must prove the integrity of the CCTV footage, the source of the footage, the method of extraction, the device used and the authenticity of the CCTV footage. Just taking a screenshot or a set of algorithms is not enough. In the same way, when an AI tool is used to analyse a vast amount of digital information, the court needs to be aware of the data used, how it was gathered, whether it was obtained lawfully or not, whether it has been manipulated, and whether it is possible for the court to verify the output itself. But, AI-generated content needs to adhere to the regulations on digital evidence, and cannot circumvent evidentiary protections, pursuant to the existing legal framework: Bharatiya Sakshya Adhiniyam, 2023.[36]

The other procedural issue is explainability. Explainability refers to the ability of the reasons or logic behind an output produced by an AI being understood and reviewable. In the criminal justice system, there is not only a technical requirement of explainability, but also a constitutional requirement. When a person is arrested, questioned and prosecuted because of a

[35] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[36] The Bharatiya Sakshya Adhiniyam, 2023, ss. 61–63.

technological output, the person shall have the right to know the basis of the charge. The right of defence is undermined by the fact that if the result of AI is not explained, the accused is unable to effectively cross-examine an algorithm without the information of the underlying method and data, and of the human decision-making process. As a result, there is a need for courts to require that AI outputs must include information about the AI system used, the data source, the AI's confidence score, the rate of errors, the audit track, and human verifications.

Also, it is important to consider who will be held liable in the case of a vendor's harassment. Private technology firms can create, maintain, or provide many tools that law enforcement use to aid in their work. This presents a danger of the private sale of fundamental criminal justice tasks from private vendors. If software gives a wrong answer, it is not an entirely vendor's problem. Policing is a sovereign function, and the State's use of its tools is a constitutional responsibility, which means that any deprivation of freedom of movement is a state responsibility. But the vendors should not be spared from being examined. Agreements on AI policing tools should mandate accuracy, auditing, testing for bias, data security, disclosure, and responsibility for faulty systems. The public law responsibility cannot end simply because a technological system was "privately developed.

The role of the police is also crucial. The use of AI should be to aid, not replace, the use of independent legal judgment by police officers. Just because an algorithm "matches" or creates an alert, that isn't enough of a basis for an arrest or detention by a police officer. All the officer has to do is determine if there is reasonable suspicion, lawful authority, corroborative material and procedural compliance on his or her own. The same is true for the exercise of police powers by using Artificial Intelligence, which has to be subject of procedural safeguards and accountability, in accordance with D.K. Basu v. State of West Bengal.[37] Technological tools must not be used as a cover for unlawful measures. All coercive measures have to be traceable back to a responsible human decision maker.

Remedies are also at the heart of this issue. The face recognition technology was wrongly used by a law enforcement agency in a particular case, the predictive policing technology misidentified a specific group of individuals, and an individual was arrested because of a false result from an AI system — there must be remedies. They can range from rectifying records, erasing incorrect biometric data, explaining decisions, departmental investigations, to settling

[37] D.K. Basu v. State of West Bengal, (1997) 1 SCC 416.

the cost of wrongful arrest or harassment, and having an AI decision reviewed by court. If there are no remedies, the constitutional rights are only empty words. Not only is it essential that the right to be free from unlawful deprivation of liberty be upheld, but also that there be meaningful redress when the right to liberty, to dignity or to privacy is infringed.

So, the results produced by AI should be used as tools for investigation and not as final determinations. They can assist an investigation with evidence, compile information, assist police in tracking down suspects or cull through digital information; but cannot be used in a prosecution without further independent evidence. Facial recognition matches shall be supported by evidence of a witness, CCTV, location, forensic material, recovery evidence or other legally admissible evidence. Predictive policing alerts should never be an arrest, detention, search or interrogation on their own. It is the constitutional responsibility to make it clear that AI should aid in investigation, but guilt should be proven in lawful, reliable, and contestable evidence. Thus, four crucial elements for the constitutionally sound application of AI in the criminal justice context are procedural fairness, evidentiary reliability, human accountability, and effective remedies.

7. Towards a Constitutional Framework for AI in Criminal Justice

Using AI in criminal justice doesn't just have to be evaluated in terms of advancement of technology or ease of administration. Policing and criminal investigation are also critical to all the rights of liberty, privacy, dignity and fair trial, and therefore should be regulated by a constitutional framework. The question is not whether the State can utilise technology for crime prevention but whether it does so within the bounds of the law, within the boundaries of proportionality, be open and transparent, and be fair and accountable. An efficient criminal justice system under a democracy cannot be run at the expense of constitutional protections. Hence, a rights-based legal regime for regulating predictive policing, facial recognition, automated surveillance and AI-assisted investigation is necessary in India.

The first condition of the same is legality. Article 21 allows for deprivation of life or personal liberty only in accordance with a procedure established by law, and the Supreme Court has defined such procedure to mean a fair, just and reasonable procedure. AI-based policing should, therefore, not be based on mere executive instructions, police circulars, pilot projects or private vendor arrangements. The technology should be clearly defined by existing legislation, the use of the technology should be defined by existing legislation, the authority competent to give

approval for the use of the technology should be clearly defined by existing legislation, the type of data to be processed should be clearly defined by existing legislation, the persons for whom the data may be provided should be clearly defined by existing legislation, and the remedies available should be clearly defined, in case of misuse, by existing legislation. If there is no specific legal justification, technologies like face recognition and predictive policing can lead to a violation of personal liberty and privacy in an arbitrary fashion.[38]

The other requirement is necessity and purpose limitation. AI tools in criminal justice should be used only for purposes of investigation of serious offences, identification of missing persons, tracing of absconding accused persons or analysis of legally collected evidence. They should not be used for blanket social surveillance, routine checks on mundane people or for constant surveillance of public areas. The element of purpose limitation is of special significance because data gathered for one purpose may be used for another. For instance, a database for missing children should not be made available as a general policing database without the law's permission and adequate safeguards. The Digital Personal Data Protection Act, 2023 recognizes the need for regulation of processing of digital personal data, but the use of AI in criminal justice needs more specific sectoral regulation as it could impact the liberty of an individual.[39]

The Digital Personal Data Protection Act, 2023 is India's first comprehensive data protection statute, and it establishes a broadly consent-based regime under which a "Data Fiduciary" processing the "personal data" of a "Data Principal" must generally obtain informed consent, adhere to purpose limitation and data minimisation, and provide notice of the purpose of processing, subject to the rights of correction, erasure and grievance redressal available to the individual whose data is processed.[40] On its face, this framework would appear to discipline the collection and use of biometric and behavioural data that predictive policing and facial recognition depend upon.

However, Section 17(1)(c) of the Act exempts processing of personal data that is "in the interest of prevention, detection, investigation or prosecution of any offence" from almost all of the Act's core obligations, including consent, purpose limitation and notice requirements.[41]

[38] Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
[39] The Digital Personal Data Protection Act, 2023; Ministry of Electronics and Information Technology, Government of India, The Digital Personal Data Protection Act, 2023 (2023).
[40] The Digital Personal Data Protection Act, 2023, ss. 4-8.
[41] The Digital Personal Data Protection Act, 2023, s. 17(1)(c).

Separately, Section 17(2)(a) empowers the Central Government to notify any instrumentality of the State as wholly exempt from the Act on grounds of sovereignty, security of the State, public order or friendly relations with foreign States, without prescribing any independent oversight, sunset clause or judicial review akin to what this Court itself had read into surveillance law in PUCL.[42] Consequently, police departments deploying predictive policing tools or facial recognition systems for investigative purposes may lawfully fall outside most of the Act's protective architecture precisely at the point where the risk to liberty is highest.

This is the precise regulatory gap that the constitutional analysis above seeks to close. A general data protection statute, however comprehensive, cannot substitute for sector-specific legislation on AI-based policing, because Puttaswamy's four-part test of legality, legitimate aim, necessity and proportionality demands calibrated safeguards, such as purpose limitation specific to serious offences, defined retention periods, independent audit and a reviewable authorisation process, that Section 17's blanket exemptions do not, by themselves, supply.

The third is proportionality. To satisfy the legality, legitimate aim, necessity and proportionality test, the State must demonstrate the necessity of this activity for a specific criminal justice purpose as well as the fact that the same objective could not reasonably be achieved without the use of AI. The rigor should be proportional to the intrusion. A targeted facial recognition search conducted in a particular investigation might be more easily justified than continuous real-time facial recognition of everyone in a public space. In a similar manner, crime mapping to allocate internal resources could be less intrusive than person-based predictive policing, which can classify people as potential criminals.[43]

The fourth one is transparency and explainability. The use of AI systems in criminal justice should not be a black box. When the consequences of a technical output involve an individual's freedom, reputation or legal situation, the individual involved should have a real possibility to be informed and contest the grounds for the technical use. Simply providing all technical aspects of the algorithm to the public would not necessarily be considered transparency, but ensuring the purpose of the algorithm, sources of data, error rates, audit results, confidence thresholds, human verification process, and limitations are disclosed would be considered transparency. Explainability is critical as judges, lawyers, accused persons and police officers

[42] The Digital Personal Data Protection Act, 2023, s. 17(2)(a).
[43] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

must be able to determine the reliability, bias, out-of-date, or legal irrelevance of an AI output.

The fifth requirement is Independent Audit and Bias testing. AI systems are only as reliable as the data that they're built out of. The algorithm can perpetuate inequalities if they exist in history in the policing of certain areas or are caused by social bias.The algorithm can perpetuate inequalities if there are inequalities that have existed in history with regards to the policing of certain areas, or as a result of social bias. So, facial recognition and predictive policing systems need to be independently audited on a regular basis. Those audits should include accuracy, false positives, false negatives, demographic bias, database quality, data retention and impact on vulnerable groups. If not auditable, AI can have the aura of a scientific solution to constitutionally illegitimate discrimination.

Human supervision is the sixth requirement. But AI cannot be used to replace human judgment in criminality. An algorithmic prediction and/or facial recognition match should not be the sole basis for arrest, detention, search, interrogation, or prosecution of any person. A responsible police officer needs to do an independent evaluation of the material, to record the reasons, to verify the output and to ensure that the material is compliant with legal safeguards. This is a requirement because of the context, discretion, proportionality and constitutional responsibility involved in making decisions in the field of criminal justice. The State will not be able to pass on the responsibility to a software system or a private vendor. Human intervention ensures accountability is with legally appointed authorities.

Evidenced control is the 7th requirement. AI generated answers should be used as investigative leads, rather than as conclusive evidence. Independent evidence (witness evidence, CCTV chain of custody evidence, forensic material evidence, location evidence, recovery evidence and/or other admissible evidence) must support a facial recognition match. Likewise, predictive policing should not be the sole basis to arrest or detain. These principles underscore the need to consider digital evidence as part of a process that ensures its authenticity and reliability before it can be used in court, otherwise digital evidence could bear no evidentiary burden.[44]

The eighth requirement is for accountability and remedies. There should be effective remedies for those who are wrongly identified, subject to surveillance, arbitrarily detained or whose reputation is damaged by police actions based on AI. They can involve disclosure of the use of

[44] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

AI, correcting or removing errors, taking action on responsible officers, conducting an independent investigation, compensation, and judicial review. If there is no action that is actually taken to enforce then constitutional rights are meaningless. All AI policing systems should, as a result, have audit logs, decision logs, approval logs, and data access logs, and be able to determine the responsibility if they are misused.

Comparative frameworks can give pointers for India.[45] These approaches reveal that the governance of AI can no longer rely solely on voluntary ethics and that certain AI uses, such as law enforcement and biometric identification systems, need to be strictly regulated, supervised, and safeguarded through institutions and laws.[46]

The demand in India isn't for the complete ban on AI in criminal justice, rather it's for constitutional regulation. Police departments could potentially use AI to analyse data, help identify crime trends, track down missing persons and organize evidence. But such use has to be subordinate to Article 21. While the Constitution is not anti-innovation, it does mandate respect for liberty, dignity, privacy, equality, due process in the context of innovation. In the end, it can be said that while AI in criminal justice is not inherently unconstitutional, unregulated AI poses a constitutional threat. Predictive policing, facial recognition and AI-assisted investigation are subject to a principle of legality, necessity, proportionality, transparency, accountability, human oversight, and effective remedies. Technological development can only be harmonized with the rule of law, with the basic rights guaranteed by Article 21, once.

8. Conclusion

This paper set out to examine whether the use of Artificial Intelligence in the criminal justice system, particularly predictive policing and facial recognition technology, can be reconciled with Article 21 of the Constitution of India. The analysis shows that AI is not inherently unconstitutional in the field of policing, but its unregulated and opaque use carries a real constitutional cost. Predictive policing risks converting statistical correlation into algorithmic suspicion, facial recognition risks enabling mass, generalised surveillance of persons who are not suspected of any offence, and both risk entrenching historical bias under the appearance of

[45] European Commission, AI Act: Regulatory Framework on Artificial Intelligence (2024).
[46] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).

neutral technology.

The constitutional jurisprudence surveyed in this paper, from Maneka Gandhi and Puttaswamy to PUCL, Selvi, D.K. Basu and Anuradha Bhasin, consistently demands that any State action affecting liberty be legal, necessary, proportionate, transparent and accountable. Applied to AI-based policing, this jurisprudence translates into concrete safeguards: a specific statutory basis rather than executive circulars or vendor pilots; purpose limitation to serious, defined offences; independent bias audits; mandatory human verification before any coercive action; and enforceable remedies for wrongful identification or surveillance. The Digital Personal Data Protection Act, 2023, though a welcome first step in India's data governance, is not a substitute for this sectoral regime, since its law-enforcement exemptions under Section 17 leave precisely the AI-policing use cases that carry the greatest risk to liberty outside meaningful oversight.

The demand emerging from this study is accordingly not for a ban on AI in criminal justice but for its constitutional domestication. Police departments can legitimately use AI to analyse data, identify crime trends, trace missing persons and organise evidence, provided such use remains subordinate to Article 21 rather than a substitute for it. The Constitution is not opposed to technological innovation; it is opposed to innovation that escapes legality, proportionality and accountability. AI-assisted investigation, predictive policing and facial recognition can only be harmonised with the rule of law once they are treated as aids to human judgment and evidence, and not as autonomous grounds for arrest, detention or guilt. A rights-based statutory framework for AI-driven policing is, therefore, not a constraint on effective law enforcement in India but a precondition for it.

Bibliography

Statutes

- The Constitution of India, arts. 14, 19 and 21.
- The Bharatiya Sakshya Adhiniyam, 2023.
- The Digital Personal Data Protection Act, 2023.

Cases

- Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.
- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- D.K. Basu v. State of West Bengal, (1997) 1 SCC 416.
- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
- Selvi v. State of Karnataka, (2010) 7 SCC 263.
- Shreya Singhal v. Union of India, (2015) 5 SCC 1.

Government and Institutional Reports

- European Commission, AI Act: Regulatory Framework on Artificial Intelligence (2024).
- Ministry of Electronics and Information Technology, Government of India, The Digital Personal Data Protection Act, 2023 (2023).
- Ministry of Home Affairs, Government of India, "Automated Facial Recognition System will facilitate better identification of criminals, unidentified dead bodies and missing/found children and persons," Press Information Bureau, 4 March 2020.
- Ministry of Home Affairs, Government of India, "CCTNS Digital Police Portal Launched to Fast-track Criminal Justice Delivery," Press Information Bureau, 6 October 2017.

- Ministry of Home Affairs, Government of India, "Inter-Operable Criminal Justice System," 13 September 2024.
- Ministry of Home Affairs, Government of India, "New Features/Uses for Police Investigation in CCTNS/ICJS," 12 April 2023.
- National Informatics Centre, Government of India, "e-Prisons."
- NITI Aayog, Responsible AI for All: Adopting the Framework — A Use Case Approach on Facial Recognition Technology (Government of India, 2022).
- Supreme Court of India, e-Committee, "e-Prisons," 28 August 2020.
- UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021).
- Vidhi Centre for Legal Policy, "India's Tryst with Predictive Policing," 13 April 2020.

Books and Articles

- Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York University Press, 2017).
- Rashida Richardson, Jason M. Schultz and Vincent M. Southerland, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," 94 New York University Law Review Online 192 (2019).