Predictive Criminal Justice: Expanded Legal Analysis of AI Systems Used to Predict Crime and Criminal Behavior

العدالة الجنائية التنبؤية: تحليل قانوني موسع لأنظمة الذكاء الاصطناعي المستخدمة للتنبؤ بالجريمة والسلوك الإجرامي



Tayeb Belouadah [1*]

[1] Faculty of Law and Political Sciences, University of M'sila, Algeria

tayeb.belouadah@univ-msila.dz

https://orcid.org/0000-0002-7404-5872

Date of transmission: 02/03/2026 date of acceptance: 25/05/2026 date of publication: 01/06/2026

****

Abstract:

Predictive criminal justice describes the use of artificial intelligence and statistical algorithms to forecast crime, assess individual "risk," and guide decisions in policing, pretrial release, sentencing, corrections, and supervision. While advanced analytics may enhance consistency and resource allocation, these systems raise acute rule-of-law concerns because their outputs can function as grounds for coercive state action. Training data frequently reflect unequal enforcement patterns and underreporting, enabling feedback loops that intensify surveillance in already over-policed communities and reproduce discriminatory effects through proxy variables even where protected traits are excluded. Model opacity, trade-secret claims, and technical complexity may impair disclosure, adversarial testing, and judicial oversight, thereby undermining due process and the right to a meaningful challenge. The principal legal issue is whether probabilistic forecasts can be reconciled with constitutional standards of individualized suspicion, the presumption of innocence, transparency, accountability, and non-discrimination, or whether legality requires stringent statutory limits, auditing, and effective remedies.

key words: Predictive; Criminal; Justice; AI Systems.

الملخص :

تسعى «العدالة الجنائية التنبؤية» إلى توظيف الذكاء الاصطناعي والخوارزميات الإحصائية للتنبؤ بالجريمة وتقييم مستوى خطورة الفرد، وتوجيه قرارات الضبطية القضائية والإفراج قبل المحاكمة وإدارة السجون والرقابة اللاحقة وغيرها، ومع أن التحليلات المتقدمة قد تعزّز التناسق وحسن توزيع الموارد، فإن هذه النظم تثير إشكالات جسيمة تتصل بسيادة القانون لأن مخرجاتها قد تُعامل كأساس لإجراءات قسرية من جانب الدولة. وغالباً ما تعكس بيانات التدريب أنماطاً غير متكافئة في إنفاذ القانون بما يتيح حلقات تغذية راجعة تُكثّف الرقابة في المجتمعات الأكثر استهدافاً وتعيد إنتاج آثار تمييزية. كما قد تؤدي عتمة نماذج الذكاء الاصطناعي إلى إضعاف حقوق المتهم بما يمس ضمانات المحاكمة العادلة وحق الدفاع.

الكلمات المفتاحية: التنبؤ، القانون الجنائي، العدالة، أنظمة الذكاء الاصطناعي

* **Corresponding Author**

Introduction:

Predictive criminal justice refers to the integration of artificial intelligence ("AI") and machine-learning ("ML") algorithms into the institutions that investigate, prosecute, adjudicate, and punish crime. In its most operational form, it involves forecasting where crime is likely to occur, estimating whether a person is likely to be arrested or convicted again, fail to appear, or violate supervision, and inferring patterns of criminal behavior from large-scale data—often drawn from police records, court files, correctional databases, and increasingly, commercially sourced information. These tools are frequently promoted as neutral technologies of efficiency: they promise to replace intuition with evidence, to reduce inconsistency, and to enable preventive allocation of scarce resources. However, because the outputs of predictive systems are used to shape patrol patterns, investigative targeting, detention decisions, sentencing outcomes, and supervision intensity, predictive criminal justice is not merely an administrative innovation. It is a form of state decision-making that can restrict liberty, intensify surveillance, and redistribute the burdens of criminal justice—often without the transparency and contestability that legality requires.

The central problem is that prediction in criminal justice is never purely technical. AI systems learn from historical data that reflects human choices: what communities were policed most aggressively, which offenses were prioritized, which incidents were recorded, how crimes were classified, and how prosecutorial discretion was exercised. The resulting datasets are therefore not a neutral measure of "crime" but a measure of recorded crime and recorded enforcement. When predictive tools are trained on these data and then used to direct future enforcement, they risk creating self-confirming feedback loops: heightened policing generates more stops and arrests, which generates more data, which in turn "validates" the algorithm's risk designation. At the same time, the opacity of complex models and the protection of proprietary systems as trade secrets may prevent defendants and courts from understanding, testing, or effectively challenging algorithmic outputs—despite the fact that those outputs can materially affect detention, sentencing, and supervision. These dynamics raise acute concerns under due process, equality and non-discrimination norms, privacy and surveillance constraints, and the foundational premise that coercive state action must be justified by reasons capable of scrutiny.

This article argues that predictive criminal justice must be evaluated not only by its claimed utility, but by whether it can be reconciled with the rule of

law. It therefore treats algorithmic prediction as a legal object: a decision-making instrument that must be authorized, intelligible, reviewable, and constrained. To that end, the analysis is divided into the following Section:

Section One: The Architecture of Predictive Criminal Justice: Systems, Rationales, and Structural Risks.

Section Two: Predictive Tools Under Law: Constitutional Constraints, Procedural Guarantees, Equality Norms, and Rule-of-Law Safeguards.

By structuring the discussion in this way, the article treats predictive criminal justice as a fundamental question of legal legitimacy: whether a system premised on probabilistic forecasts can be integrated into coercive state practice without sacrificing transparency, equality, and the procedural integrity that distinguishes lawful governance from mere risk management.

Section One: The Architecture of Predictive Criminal Justice: Systems, Rationales, and Structural Risks

I. Taxonomy: Where Prediction Enters the Criminal Process

Although "predictive justice" is often discussed as a single phenomenon, it is more accurately understood as a set of distinct interventions that arise at different procedural stages and therefore engage different legal standards.

A. Predictive Policing (Place-Based Forecasting)

These systems attempt to estimate where certain crimes are likely to occur, typically using historical police data (incident reports, arrests, calls for service), spatiotemporal patterns, and sometimes environmental variables.[1] Place-based models frequently present their output as "hot spots," "risk terrain," or patrol boxes. Even when the model's unit is geographical, the downstream consequences are personal: increased patrol in a hot spot increases stops, field interrogations, searches, and low-level arrests.[2] This triggers Fourth Amendment (or analogous) concerns about the transformation of probabilistic, population-level correlations into individualized suspicion.[3]

---

[1] United States Department of Justice, Office of Community Oriented Policing Services, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations (2013). p.18.

[2] National Research Council, Fairness and Accuracy in Statewide Pretrial Prediction (National Academies Press 2019). p.24.

[3] Sandra G Mayson, 'Bias In, Bias Out' (2019) 128 *Yale Law Journal* 2218. p.64

B. Person-Based Systems (Risk Scoring)

Risk assessment tools operate in pretrial, sentencing, parole, and probation contexts, typically aiming to predict recidivism, failure to appear, or supervision violations.[1] These tools sometimes rely on criminal history, age, employment, housing stability, education, and other "criminogenic needs" variables.[2] Person-based predictions implicate due process, equal protection, and the legality of basing liberty decisions on correlations with group traits rather than individualized culpability.[3]

C. Investigative Analytics and "Suspicion Infrastructure."

Some agencies use link analysis, social network analysis, facial recognition, and data fusion (including third-party commercial data) to infer associations, identify "persons of interest," or prioritize investigative targets.[4] While often framed as mere triage, these systems can operate as a suspicion-generating infrastructure, creating investigative leads that may later be laundered into ostensibly independent grounds for stops, warrants, or arrests.[5] The legal danger is not simply error, but the erosion of traceability and accountability: if the state cannot later disclose how an investigation began, adversarial testing becomes illusory.[6]

II. The Data Problem Is a Legality Problem

Predictive systems are commonly described as "data-driven," but in criminal justice the data itself is frequently a product of discretionary enforcement practices. Crime data does not measure crime in the abstract; it measures, what is reported, what police record, what police choose to enforce, and how agencies classify and code events. Underreporting is pervasive, particularly for sexual violence, domestic abuse, and crimes in communities with low trust in law enforcement.[7] Arrest and stop data, meanwhile, reflects patrol patterns and

---

[1] Cynthia Rudin, 'Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead' (2019) 1 Nature Machine Intelligence 206. p.78.

[2] Danielle Keats Citron, 'Technological Due Process' (2008) 85, *Washington University Law Review* 1249. p.41.

[3] Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015). p.34.

[4] Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (NYU Press 2017).

[5] Richard Berk, Artificial Intelligence and the Criminal Justice System (Academic Press/Elsevier 2019).

[6] National Research Council (n 6). op.cit. p. 12.

[7] Richard Berk, Artificial Intelligence and the Criminal Justice System (Academic Press/Elsevier 2019). p. 18.

enforcement intensity, which vary significantly across neighborhoods and social groups.[1]

This produces a fundamental legal tension: when the state uses enforcement-produced data to justify future enforcement, the state risks circular reasoning. In effect, prior enforcement becomes evidence of future risk, which becomes the justification for intensified enforcement, thereby generating additional enforcement data that "validates" the original risk designation.[2] This feedback loop is not merely a technical artifact; it can operate as a self-fulfilling governance mechanism that entrenches unequal policing burdens.[3]

Moreover, the use of proxy variables can replicate discrimination without explicit classification. Even when race is formally excluded, variables such as neighborhood, prior police contacts, and employment instability may correlate with race and poverty due to structural inequalities and historical over-policing.[4] Anti-discrimination law has long recognized that facial neutrality does not preclude disparate impact, especially where unequal burdens are foreseeable and avoidable.[5] In this respect, algorithmic "race blindness" can be a compliance strategy that fails to address substantive inequality.[6]

III. Predictive Policing and the Fourth Amendment: From Probability to Suspicion

Predictive policing raises acute Fourth Amendment concerns because it encourages a conceptual slide from generalized probability to individualized suspicion. Hot-spot forecasting may be legitimate as a resource-allocation tool; yet, when officers treat presence in a predicted zone as a justification for heightened intrusions (stops, frisks, searches), the algorithm's statistical output begins to function as an ersatz substitute for the individualized facts required by constitutional doctrine.

The doctrinal difficulty is that Fourth Amendment standards such as "reasonable suspicion" and "probable cause" demand particularized and objective justification grounded in articulable facts about the person to be seized or

---

[1] Bernard E Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age (University of Chicago Press 2007). p. 25.
[2] Citron, op.cit. p. 42.
[3] Mayson, op.cit (n 7). p. 65.
[4] Rashida Richardson, Jason M Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 *NYU Law Review Online*. p.15.
[5] Andrew Guthrie Ferguson, op. cit. p. 24.
[6] Kristian Lum and William Isaac, 'To Predict and Serve?' (2016) 13(5) *Significance*.p.14.

searched.[1] Algorithmic forecasts are typically aggregate correlations: they speak to a place or class, not to a specific individual's conduct at a specific moment. If agencies operationalize hot-spot predictions as permission for aggressive pedestrian or vehicle interdiction, they risk converting whole neighborhoods into de facto "suspicion zones," a practice historically condemned when implemented through less technological means.[2]

Predictive systems also affect warrant practice. If algorithmic analytics are used to develop leads, and those leads are not disclosed in warrant affidavits (either because officers view them as "non-evidentiary" or vendors claim secrecy), the defense may be deprived of the ability to challenge whether the warrant was supported by lawful and sufficient grounds.[3] This concern is especially pronounced where "parallel construction" is used—i.e., where law enforcement reconstructs an alternative narrative for how a suspect was identified, obscuring the algorithmic origins.[4] Such practices undermine the integrity of judicial oversight and may implicate disclosure obligations under criminal procedure rules and constitutional due process requirements.[5]

Section Two: Predictive Tools Under Law: Constitutional Constraints, Procedural Guarantees, Equality Norms, and Rule-of-Law Safeguards

I. Pretrial Risk Assessment: Liberty Decisions Without Adjudication

Risk assessment in pretrial contexts is often justified as an alternative to cash bail and as a mechanism to reduce unnecessary detention.[6] Properly designed and constrained, pretrial tools may support decarceration by identifying low-risk defendants suitable for release.[7] Yet the legal hazard is that risk scores become a substitute for individualized judicial reasoning, and that "high risk" labels become a mechanistic rationale for detention in cases where detention should be exceptional and narrowly justified.[8]

Pretrial determinations are uniquely sensitive because they occur prior to adjudication of guilt. The presumption of innocence is not merely rhetorical; it is

[1] Richardson, Schultz and Crawford, op.cit. p. 28.
[2] Harcourt, op.cit. p. 15.
[3] Mayson, op.cit. p. 52.
[4] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review*. p. 671.
[5] Citron, op.cit. p. 71.
[6] Pasquale, op.cit. p. 25.
[7] Citron, op.cit. p. 45.
[8] Richardson, Schultz and Crawford (n 19). op.cit. p. 41.

the constitutional and moral premise that the state must not punish before conviction.[1] If risk scores are treated as quasi-evidence of dangerousness or future criminality, the state risks transforming pretrial detention into preventive incarceration. The law in many jurisdictions permits preventive detention only under strict statutory criteria and procedural safeguards; algorithmic scoring must not become a means to evade those constraints.[2]

An additional problem is calibration across groups. A tool can be "equally accurate" under one metric while still producing different false-positive rates across racial groups due to different base rates in the training data or differences in policing intensity.[3] In a liberty context, disparate false positives mean one group experiences more unjustified detention and supervision burdens, even if the tool's aggregate performance appears acceptable.[4] Where a tool's design embeds trade-offs among fairness metrics, the choice is inherently normative and must be made transparently by accountable public officials—not silently by vendors or default settings.[5]

II. Sentencing and Corrections: The Risk of Actuarial Punishment

In sentencing, the state's moral authority rests on proportional punishment for proven wrongdoing, bounded by law and individualized consideration. When risk assessment tools are introduced at sentencing, they create pressure to increase punishment for persons predicted to reoffend, thereby importing preventive logic into a context traditionally oriented toward desert and proportionality.[6] This shift raises rule-of-law concerns: punishment may become less about what was done and more about what is feared.

Correctional and supervision tools also implicate liberty and equality. Classification algorithms can affect facility placement, program access, and supervision intensity. Supervision algorithms may increase monitoring or impose restrictive conditions based on predicted risk. These measures can produce "mass supervision" dynamics—frequent technical violations, revocations, and returns to custody—driven not by new crimes[7] but by intensified surveillance and

---

[1] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press 2018). p.14.
[2] National Research Council. op.cit. p. 22.
[3] Frank Pasquale. op.cit. p. 31.
[4] Bernard E Harcourt. op.cit. p. 27.
[5] Richard Berk. op.cit. p. 29.
[6] Bernard E Harcourt. op.cit. p. 35.
[7] See. Tayeb belouadah, The Criminal Law Challenges in Confronting AI Crimes, *Algerian Journal of Law And political Sciences*, Vol 10, Issue 01(2025), p. 1159.

compliance burdens.[1] The legal question becomes whether the state may impose increasingly onerous constraints based primarily on statistical prediction, especially when the predictions themselves reflect historically unequal enforcement patterns.[2]

III. Due Process and the Right to a Meaningful Challenge

The strongest legal critique of predictive criminal justice is procedural: coercive decisions must be explainable, contestable, and reviewable. Danielle Citron's concept of "technological due process" emphasizes that when automated systems make or materially influence decisions, individuals must have notice, access to the basis of the decision, and a meaningful opportunity to contest errors.[3]

Three recurring barriers arise:

1. Trade secrecy and vendor opacity. Vendors may refuse to disclose model structure, feature weights, or training data, claiming proprietary protection.[4] When such systems influence detention or sentencing, secrecy conflicts with fundamental fairness and the right to challenge adverse evidence.[5]

2. Complexity and non-interpretability. Even when disclosed, complex models may not yield reasons intelligible to courts or defendants.[6] In criminal settings, opacity is not a benign inconvenience; it is a structural impediment to adversarial testing.

3. Data integrity problems. Criminal databases can contain errors in identity, disposition, or event coding. Without a robust right to inspect and correct data, individuals may be burdened by false records that propagate across systems.

Due process is not satisfied by mere disclosure of a final score. A numerical label ("7/10 risk") without an auditable basis is not a reason; it is an assertion. If algorithmic tools are to be used, the defense must be able to test: (i) the accuracy of input data, (ii) the relevance and legality of features, (iii) the validation evidence in the local jurisdiction, and (iv) the error characteristics across protected groups.[7]

IV. Equal Protection, Disparate Impact, and Structural Inequality

[1] Bernard E Harcourt. op.cit. p. 13.
[2] National Research Council. op.cit. p. 36.
[3] Sandra G Mayson. op.cit. p. 25.
[4] Cynthia Rudin. op.cit. p. 14.
[5] National Research Council. op.cit. p. 22.
[6] O'Neil, Cathy, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown 2016). p. 18
[7] Danielle Keats Citron, op.cit. p. 32.

Algorithmic criminal justice frequently produces disparate racial and socioeconomic impacts because it operates on data generated within unequal systems. Scholars have emphasized that bias may enter at every stage: selection of the target variable (what the tool predicts), selection and coding of input features, enforcement-generated labels, and policy thresholds determining who is classified "high risk."[1]

Disparate impact alone may not always establish constitutional violation under U.S. equal protection doctrine absent proof of discriminatory intent, but civil rights statutes, state constitutional provisions, and administrative law principles may provide additional avenues to challenge unjustified disparate effects.[2] Moreover, even within intent doctrine, the foreseeability of discriminatory effects and the refusal to adopt less discriminatory alternatives may be relevant to assessing unlawful purpose or deliberate indifference in certain contexts.[3] At minimum, equality principles demand that the state not deploy tools that predictably amplify unequal burdens without compelling justification and rigorous mitigation.[4]

V. Evidentiary Standards and the "Scientific" Aura of Risk Scores

Risk tools often benefit from a "scientific" aura that can distort legal judgment. Yet a model's statistical association does not establish causal explanation, and causation matters when the state imposes coercive constraints.[5] The law should be wary of replacing individualized evidence with actuarial inference, especially where the inference is derived from contested proxies.

Further, predictive systems embed policy choices that are often hidden: which outcomes matter (rearrest vs reconviction), what time horizon is used, what threshold triggers detention or supervision escalation, and what costs are assigned to false positives. These are not technical choices; they are normative judgments about whose liberty may be restricted to manage risk. If such judgments are made invisibly—by vendors or through default configurations—democratic accountability is impaired.

---

[1] Richard Berk. op.cit. p. 41.
[2] Frank Pasquale. op.cit. p. 22.
[3] Cynthia Rudin. op.cit. p. 57.
[4] Andrew Guthrie Ferguson, op.cit. p. 61.
[5] ibid, p.62.

VI. Governance and Legal Safeguards: Toward a Rights-Consistent Model

If predictive tools are used in criminal justice at all, legality requires enforceable guardrails. A rights-consistent governance framework should include:

1. Statutory authorization and purpose limitation. Agencies should not deploy predictive systems absent clear legal authority defining permissible purposes, prohibited uses, and procedural safeguards.[1]

2. Mandatory algorithmic impact assessments. Before adoption, agencies should publish assessments describing data sources, intended uses, expected impacts, error trade-offs, and mitigation strategies, with meaningful public consultation.[2]

3. Independent validation and continuous auditing. Tools must be tested locally, monitored for drift, and audited for subgroup error rates and disparate impact.[3]

4. Disclosure, defense access, and adversarial testing. In any liberty-affecting use, defendants must receive the score, the factors materially contributing to it, validation evidence, and a mechanism to challenge errors.[4]

5. Prohibition of determinative use and requirement of reasoned decision-making. Scores must be advisory only; decision-makers must articulate individualized reasons and must not treat algorithmic output as dispositive.[5]

6. Data quality rights. Individuals must have rights to inspect, correct, and expunge erroneous or irrelevant records, with strict retention limits.[6]

7. Remedies. Courts should have authority to order disclosure, exclude unlawfully derived evidence, and provide relief when predictive systems contribute to constitutional violations.[7]

Conclusion

Predictive criminal justice, as presently deployed, should be understood as a modality of state action rather than a neutral administrative innovation. The core findings of this analysis are fourfold. First, predictive systems are structurally dependent on historical criminal justice data that frequently reflect unequal enforcement, selective reporting, and discretionary institutional choices;

[1] Bernard E Harcourt. op.cit. p. 33.
[2] Frank Pasquale. op.cit. p. 19.
[3] National Research Council. op.cit. p. 20.
[4] Danielle Keats Citron, op.cit. p. 39.
[5] Solon Barocas and Andrew D Selbst. op.cit. p. 41.
[6] Cynthia Rudin. op.cit. p. 61.
[7] Rashida Richardson, Jason M Schultz and Kate Crawford, op.cit. p. 29.

the resulting models can therefore reproduce and legitimate those disparities under the appearance of technical objectivity. Second, place-based forecasting and person-based risk scoring risk converting population-level correlations into individualized suspicion or liberty restrictions, thereby straining constitutional standards governing reasonable suspicion, due process, and the presumption of innocence. Third, opacity—whether arising from technical complexity, deficient documentation, or vendor trade-secret claims—can impair disclosure, adversarial testing, and judicial oversight, undermining procedural fairness and the ability to correct errors. Fourth, even where aggregate performance is claimed, predictive tools often embed unarticulated normative judgments (choice of outcomes, thresholds, error trade-offs) that properly belong to transparent, democratically accountable decision-making.

In light of these results, the legally sustainable path forward is not unconditional adoption, but rights-centered governance. The following measures are the principal recommendations:

Clear statutory authorization and purpose limitation. Predictive tools should be deployed only pursuant to explicit legislation or binding regulation that defines permissible use-cases, prohibits impermissible uses (including any determinative reliance in liberty-depriving contexts), and requires documented necessity and proportionality.

Mandatory transparency and disclosure in liberty-affecting decisions. Where an algorithmic output is used in pretrial, sentencing, or supervision decisions, affected persons must receive timely notice, the output itself, the material factors driving it, and access to validation studies and known limitations. Trade-secret protections must yield where they defeat due process.

Independent validation, continuous auditing, and public reporting. Agencies must conduct local validation prior to deployment and continuous monitoring thereafter, including subgroup error-rate analysis, disparate impact assessments, and drift detection. Audit results and performance metrics should be published in accessible form, subject only to narrowly tailored security exceptions.

Data governance, integrity rights, and minimization. Jurisdictions should adopt enforceable rules governing data quality, provenance, retention, sharing, and security; individuals should have practical mechanisms to inspect and correct erroneous records. Sensitive attributes and proxy variables must be controlled, and non-essential data should not be collected or retained.

Procedural safeguards against automation bias. Algorithmic outputs must be advisory, not dispositive. Decision-makers should be required to provide individualized reasons on the record and to document the weight given to algorithmic tools, ensuring that human judgment remains accountable and reviewable.

Judicial capacity and evidentiary standards. Courts should develop standards for admitting or relying upon algorithmic assessments, including requirements of explainability, demonstrable validity for the relevant population, and transparency sufficient for adversarial testing. Where algorithmic practices contribute to unlawful searches, seizures, or detentions, effective remedies—including exclusion where appropriate—must be available.

Moratoria or prohibitions where legality cannot be secured. In high-stakes contexts—particularly predictive policing practices that operationalize hot-spot forecasts as a basis for stops or that rely on undisclosed data fusion—jurisdictions should impose moratoria unless and until compliance with constitutional requirements, robust oversight, and meaningful contestability can be demonstrated.

The overarching recommendation is thus one of conditional legitimacy: predictive technologies may be permissible only where they are strictly bounded by law, transparent in operation, empirically validated, and fully contestable, and where they do not function as a substitute for individualized suspicion, proof, or reasoned judicial determination. Absent these safeguards, predictive criminal justice is likely to amplify unequal burdens, erode procedural integrity, and weaken public confidence in the fairness of the criminal legal system—outcomes incompatible with the rule of law.

List of sources and references:

1. Andrew Guthrie Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (NYU Press 2017).
2. Bernard E Harcourt, Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age (University of Chicago Press 2007).
3. Cynthia Rudin, ‘Stop Explaining Black Box Machine Learning Models for High Stakes Decisions and Use Interpretable Models Instead’ (2019) 1 Nature Machine Intelligence 206.
4. Danielle Keats Citron, ‘Technological Due Process’ (2008) 85 Washington University Law Review 1249.

5. Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Harvard University Press 2015).
6. Kristian Lum and William Isaac, 'To Predict and Serve?' (2016) 13(5) Significance 14.
7. National Research Council, Fairness and Accuracy in Statewide Pretrial Prediction (National Academies Press 2019).
8. O'Neil, Cathy, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (Crown 2016).
9. Rashida Richardson, Jason M Schultz and Kate Crawford, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (2019) 94 NYU Law Review Online 15.
10. Richard Berk, Artificial Intelligence and the Criminal Justice System (Academic Press/Elsevier 2019).
11. Sandra G Mayson, 'Bias In, Bias Out' (2019) 128 Yale Law Journal 2218.
12. Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.
13. Tayeb belouadah, The Criminal Law Challenges in Confronting AI Crimes, Algerian Journal of Law And political Sciences, Vol 10, Issue 01(2025).
14. United States Department of Justice, Office of Community Oriented Policing Services, Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations (2013).
15. Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (St Martin's Press 2018).