From Probable Cause to Predictive Cause: AI, Policing, and the Erosion of Reasonable Suspicion

1. Laraib Fatima; Research Scholar-LLB (Punjab University), MPhil (Government College University), Lahore, Pakistan.
2. Ethan Reynolds-LLB (London School of Economics), LLM (Columbia Law School, USA), Research Fellow (University of Warwick).
3. Hannah Robinson-BA (Jurisprudence, University of Oxford), LLM (University of Melbourne, Australia).

SUBMISSION DATE:
DEC 13, 2024

ACCEPTANCE DATE:
DEC 17, 2024

PUBLICATION DATE:
DEC 28, 2024

Abstract

The progressive entanglement of Artificial Intelligence (AI) with contemporary policing represents one of the most profound transformations in criminal procedure since the institutionalization of probable cause. Predictive policing systems—trained on large historical datasets—now operate as algorithmic arbiters of suspicion, displacing human judgment with computational projections of criminality. This paper interrogates how AI-driven systems redefine the constitutional standards of reasonable suspicion and probable cause under U.S. law, while simultaneously unsettling European conceptions of proportionality and necessity under the Charter of Fundamental Rights of the European Union. Drawing from interdisciplinary research in law, computer science, and philosophy, it analyzes the emergence of "predictive cause" as a new epistemic standard, rooted in algorithmic immutability and opaque reasoning. The article exposes how immutable algorithmic classifications perpetuate systemic discrimination, undermining the procedural fairness and transparency central to due process. Comparative inquiry reveals that while the U.S. leans toward operational efficiency, the E.U. foregrounds human dignity and data protection, yet both face difficulties ensuring accountability. The study concludes with doctrinal and policy recommendations aimed at reconciling algorithmic accuracy with constitutional integrity, advancing a framework for algorithmic accountability that restores the balance between technological progress and civil rights.

Keywords

Artificial Intelligence; Algorithmic Governance; Constitutional Law; Predictive Policing; Reasonable Suspicion; Due Process; Algorithmic Bias; Data Protection; Civil Rights; AI Regulation; Probable Cause; Legal Personhood.

Introduction

The diffusion of Artificial Intelligence into law enforcement has restructured the epistemology of suspicion itself. Traditional policing, governed by constitutional principles such as *probable cause* and *reasonable suspicion*, relied on individualized judgment tempered by experience and accountability. However, in the post-digital era, policing has shifted toward algorithmic forecasting—systems that claim to *predict* where and by whom crimes will occur. These systems, from PredPol to HunchLab, increasingly influence patrol deployment, surveillance intensity, and prosecutorial decision-making [1]– [3]. The question confronting jurists and policymakers is not whether such technologies are effective, but whether their predictive logic is *legally intelligible* and *constitutionally permissible*.

At the heart of this transformation lies a subtle but profound shift—from evidentiary cause to predictive cause. Probable cause, enshrined in the Fourth Amendment, demands articulable facts that would lead a reasonable officer to believe a crime has been, is being, or will be committed [4]. Predictive cause, by contrast, substitutes historical data correlations for present observation. It relies not on human inference, but on statistical learning that extrapolates risk across time and demography. The result is a hybrid form of reasoning that simultaneously amplifies precision and obscures accountability.

This evolution implicates several constitutional doctrines: due process under the Fifth and Fourteenth Amendments, equal protection, and the prohibition against unreasonable searches and seizures. Courts, from *Terry v. Ohio* (1968) to *Illinois v. Gates* (1983), have long balanced state power with individual liberty, emphasizing the *reasonableness* of police conduct. Yet algorithmic systems erode this equilibrium by delegating discretion to models that learn patterns of past enforcement, embedding the biases of prior policing [5], [6]. In this sense, predictive policing transforms suspicion from an *individualized assessment* into a *probabilistic classification*.

Scholars have argued that algorithmic immutability—the tendency of AI models to reproduce their learned patterns—renders them incapable of evolving beyond the biases of their training data [7]. Once embedded, these biases ossify into self-reinforcing loops: areas labeled as "high-risk" receive more police attention, generating more arrests, which then validate the model's assumptions. This paper contends that such immutability constitutes a structural violation of the principles of fairness, transparency, and accountability foundational to constitutional governance.

Literature Review

Academic discourse on predictive policing and AI in criminal justice has expanded rapidly since the early 2010s. Foundational works such as Ferguson's *The Rise of Big Data Policing* (2017) and Brayne's ethnographic study *Predict and Surveil* (2020) contextualize predictive algorithms within broader systems of social control [8], [9]. These analyses show that data-driven policing does not merely optimize law enforcement efficiency—it redefines the ontological basis of criminal suspicion. Instead of human intuition, predictive models rely on the statistical association of location, demography, and prior arrests.

Legal scholars such as Danielle Citron [10], Andrew Guthrie Ferguson [11], and Elizabeth Joh [12] have criticized these systems for undermining due process by introducing unreviewable algorithmic logic into decision-making. Citron's theory of "technological due process" asserts that administrative fairness requires transparency in automated systems. Similarly, Selbst and Barocas argue that fairness cannot be achieved merely by removing biased variables but requires interrogation of the *structural assumptions* that underlie data collection itself [13]. Such scholarship frames AI immutability as a procedural problem, not just a technical one.

Empirical research further substantiates the discriminatory impacts of predictive models. Lum and Isaac (2016) demonstrated that geographic prediction systems disproportionately targeted minority neighborhoods, reflecting patterns of historical over-policing [14]. Angwin et al.'s analysis of the COMPAS system revealed racial disparities in risk assessment scores, with African American defendants more likely to be labeled as high risk [15]. These findings reveal that algorithmic "objectivity" masks entrenched inequalities, translating them into mathematical form.

Philosophical and sociological contributions complement these critiques. O'Neil's *Weapons of Math Destruction* (2016) popularized the notion that algorithms can amplify injustice when optimized for efficiency rather than equity [16]. Likewise, Kate Crawford and Trevor Paglen's work on "excavating AI" exposes the cultural and epistemic assumptions encoded in training datasets [17]. Their insights underscore that AI systems are not neutral instruments but socio-technical assemblages that reproduce human hierarchies.

Within constitutional jurisprudence, the tension between predictive analytics and the Fourth Amendment has generated a growing body of case law and commentary. Legal analyses, such as those by Kroll et al. [18], raise questions about whether algorithmic forecasts meet the *individualized suspicion* required for searches and detentions. Courts have begun grappling with algorithmic evidence, as in *State v. Loomis* (2016), where the Wisconsin Supreme Court upheld the use of risk assessment tools in sentencing but warned against "overreliance" on their opaque logic [19].

Comparative studies illuminate divergent regulatory philosophies. The European Union's General Data Protection Regulation (GDPR) and the forthcoming AI Act enshrine human oversight and explicability as central principles [20]. By contrast, the U.S. lacks a comprehensive AI governance framework, relying instead on fragmented sectoral laws such as the Privacy Act of 1974 and state-level data protection statutes [21]. These regulatory asymmetries shape distinct approaches to algorithmic policing: the E.U. treats it as a data rights issue, while the U.S. frames it as an efficiency tool within constitutional constraints.

Finally, Ahmed Raza's 2024 study, *"Trade Secrets as a Substitute for AI Protection: A Critical Investigation into Different Dimensions of Trade Secrets,"* provides a crucial insight into the intersection of proprietary secrecy and algorithmic opacity. Raza argues that when algorithmic systems are shielded as trade secrets, they evade judicial scrutiny and public accountability, exacerbating the asymmetry between state power and individual rights [22]. His analysis underscores the legal paradox of predictive policing: the state increasingly relies on private algorithms whose operations cannot be disclosed, yet whose outputs shape liberty and justice.

1. Theoretical and Legal Framework

1.1 Constitutional Foundations: From Suspicion to Probability

The American constitutional framework governing policing is anchored in the Fourth Amendment, which protects individuals from unreasonable searches and seizures. *Reasonable suspicion* and *probable cause* emerged through judicial elaboration—particularly in *Terry v. Ohio* (1968) and *Illinois v. Gates* (1983)—as safeguards against arbitrary state intrusion. These doctrines hinge on the *reasonableness* of police belief, evaluated in light of observable facts [23]. However, the transition from human intuition to algorithmic prediction redefines what counts as "reasonable."

AI systems, particularly those employing machine learning, operate not through human reasoning but through pattern recognition. They detect statistical regularities that may have no direct causal connection to criminal conduct. As such, they generate *probabilistic correlations* rather than *factual grounds*. This epistemic distinction undermines the jurisprudential basis of probable cause, which assumes that suspicion arises from specific and articulable facts known to the officer at the time of action [24]. Predictive algorithms, by contrast, act as epistemic black boxes—producing conclusions that neither officers nor courts can meaningfully interpret.

1.2 Algorithmic Governance and Legal Epistemology

The shift toward predictive policing exemplifies a broader phenomenon of algorithmic governance—the delegation of state functions to automated systems [25]. This delegation raises fundamental questions about accountability and legality. According to Hildebrandt, algorithmic governance transforms law's logic from *normative reasoning* to *statistical correlation*, thereby eroding the performative power of legal norms [26]. When algorithms determine what is "reasonable," law ceases to be a system of human judgment and becomes a system of computational classification.

Legal epistemology must therefore adapt to a new evidentiary paradigm. Traditional rules of evidence—requiring reliability, relevance, and transparency—cannot easily accommodate machine learning models whose internal logic is opaque even to their creators. The Daubert standard, which governs expert testimony in U.S. courts, emphasizes falsifiability and peer review as criteria of admissibility [27]. Yet many predictive algorithms are proprietary, continuously updated, and resistant to independent validation. Their outputs, though treated as expert evidence, often fail to meet Daubert's transparency requirements.

1.3 The Problem of Algorithmic Immutability

Algorithmic immutability refers to the persistence of learned classifications within AI systems even after external conditions change [28]. Once trained, an algorithm internalizes correlations that become resistant to modification unless retrained on new data. In policing, this means that historical biases—over-policing of minority neighborhoods, disproportionate arrests, and skewed datasets—become embedded within the model's predictive logic. Retraining alone may not eliminate such bias, as the structural feedback loop between prediction and policing perpetuates its own validation.

This immutability challenges core constitutional principles. The due process clauses of the Fifth and Fourteenth Amendments guarantee fairness in both procedure and outcome. When decisions are made by immutable systems, individuals cannot meaningfully contest the basis of suspicion against them. Similarly, the Equal Protection Clause is undermined when algorithmic classifications create *de facto* groups— "high-risk individuals" or "suspect zones"—that correlate with race, class, or geography, without explicit discriminatory intent [29].

1.4 The Normative Dissonance Between Law and Machine Learning

The legal system is inherently discursive: its reasons through argument, evidence, and deliberation. Machine learning, by contrast, is inductive and iterative. It learns patterns without reasoning about causation or moral context. This creates what Mireille Hildebrandt calls "normative dissonance"—a conflict between law's demand for justifiability and AI's reliance on pattern-based prediction [30]. In policing, this dissonance manifests as the replacement of "reasonable suspicion" with "statistical suspicion," where probability replaces prudence.

Moreover, predictive policing undermines the *individualization* requirement central to constitutional jurisprudence. As Desai and Kroll observe, algorithmic suspicion generalizes across populations, erasing the individualized nexus between officer observation and suspect behavior [31]. This undermines the presumption of innocence by transforming potentiality into culpability—a hallmark of preemptive governance.

2. Analysis: Algorithmic Immutability and Discriminatory Impacts

2.1 The Self-Reinforcing Loop of Algorithmic Suspicion

Predictive policing relies on the premise that past crime data can forecast future criminality. Yet, as Lum and Isaac demonstrated, historical datasets are not neutral; they reflect decades of biased law enforcement practices [14]. When algorithms learn from such data, they internalize systemic inequities and project them forward. Police are then redeployed to the same neighborhoods, producing more arrests that validate the model's prior assumptions. This feedback loop—termed *algorithmic immutability*—ensures that predictive suspicion remains statistically accurate while normatively unjust [28].

This dynamic reframes the concept of *reasonableness* under the Fourth Amendment. In *Whren v. United States* (1996), the Court permitted pretextual stops if an objective basis for probable cause existed [32]. Algorithmic policing amplifies this logic by offering a veneer of objectivity even when the underlying correlations encode racial and socio-economic bias. Consequently, the "reasonable officer" standard mutates into a "reasonable algorithm" standard, one shielded from human accountability.

2.2 Disparate Impact and the Collapse of Intent Doctrine

Equal protection jurisprudence traditionally hinges on discriminatory intent, not merely disparate outcomes. However, algorithms operate without discernible intent—they discriminate by design, not by motive. Selbst and Barocas argue that this shift exposes a *causation gap*: machine bias produces inequality without the requisite mental state for constitutional violation [13]. Courts are thus ill-equipped to address algorithmic discrimination, since doctrines like *Washington v. Davis* (1976) require proof of intent.

Empirical studies confirm this disparity. Angwin et al. found that the COMPAS risk-assessment tool mislabeled Black defendants as high-risk nearly twice as often as white defendants with similar profiles [15]. These outcomes persist because the algorithm's features—prior arrests, neighborhood crime rates—serve as proxies for race. Algorithmic immutability prevents correction: even when biased variables are removed, correlated patterns re-emerge through other attributes such as zip code or income [33]. Thus, bias migrates within the model, evading legal detection.

2.3 Procedural Due Process and the Right to Contestability

Due process guarantees the right to know and challenge the evidence used against one's liberty interests. When predictive systems inform stops, searches, or bail decisions, defendants cannot meaningfully contest algorithmic determinations because their reasoning remains proprietary and inscrutable. This opacity violates both procedural fairness and epistemic transparency [10], [34]. The *State v. Loomis* (2016) decision illustrates this dilemma: although the court upheld COMPAS's use in sentencing, it warned that defendants must be informed of its limitations and lack of transparency [19].

Algorithmic immutability compounds this violation by freezing contestability. Because machine learning models continuously adapt to their own predictions, even post-hoc audits cannot fully reconstruct prior decision pathways. Scholars such as Kroll et al. propose "accountable algorithms" that embed auditability at the code level [18]. Yet absent statutory mandates, proprietary policing software remains shielded under trade-secret law, as highlighted by Raza (2024) [22]. The result is a constitutional asymmetry: the state may rely on secret algorithms to justify detention, while individuals are denied the means to interrogate their logic.

2.4 The Erosion of Probable Cause through Predictive Correlation

Probable cause traditionally required individualized suspicion based on observable facts. Predictive cause, however, relies on *correlated risk*. If an algorithm assigns high risk to a person based on neighborhood, social network, or past contacts with police, officers may act on that information absent direct observation. This blurs the constitutional threshold between suspicion and certainty. In *Carpenter v. United States* (2018), the Supreme Court recognized that technological surveillance requires heightened scrutiny because of its "pervasive and retroactive" reach [35]. Predictive policing extends this reach forward in time—anticipating crimes before they occur.

The jurisprudential danger is that *correlation becomes cause.* As Ferguson warns, predictive policing converts data patterns into grounds for state intervention without contemporaneous human assessment [11]. Courts may struggle to invalidate such logic when it appears statistically sound. This epistemic authority of numbers displaces the moral reasoning that once undergirded constitutional constraints. In effect, predictive algorithms operationalize a presumption of guilt by data association.

2.5 The Social Construction of Risk and Algorithmic Personhood

Beyond legal doctrines, predictive systems shape a new ontology of personhood: the individual as a *data composite*. Zuboff's theory of "surveillance capitalism" posits that predictive analytics commodify human behavior by transforming it into measurable patterns [36]. In policing, these patterns become markers of potential criminality. AI thus constructs *algorithmic identities*—immutable profiles of risk divorced from actual conduct. Such classifications reify social hierarchies under the guise of scientific neutrality.

Philosophically, this shift mirrors what Hacking termed “making up people”: categories created by data can alter how individuals are perceived and treated [37]. Once coded as high-risk, a person encounters intensified surveillance, diminished trust, and cumulative disadvantage. These algorithmic identities are self-fulfilling; they generate the very deviance they predict. Consequently, predictive policing undermines not only due process but also the constitutional ideal of equal moral worth.

3. Comparative Perspectives: United States and European Union

3.1 United States: Constitutional Minimalism and Technological Deference

The U.S. legal system approaches algorithmic policing through the prism of constitutional minimalism. The Fourth Amendment’s “reasonableness” test provides flexibility but little technological foresight. Courts have largely deferred to law enforcement claims of efficiency, applying existing doctrines without confronting algorithmic novelty [38]. In *United States v. Jones* (2012), Justice Sotomayor cautioned that prolonged GPS surveillance could “alter the relationship between citizen and government” [39]; yet predictive analytics, which operate without physical tracking, have escaped similar scrutiny.

Federal oversight remains fragmented. The Department of Justice’s 2023 guidance on AI emphasizes nondiscrimination but lacks binding enforcement mechanisms. Absent statutory limits, predictive policing is regulated primarily through Fourth Amendment litigation, where plaintiffs must show concrete injury and traceable harm—an almost impossible standard when the algorithm’s role is opaque [40]. Consequently, U.S. law privileges technological innovation over civil accountability.

3.2 European Union: Data Protection and Human Dignity

In contrast, the European Union situates algorithmic policing within a robust data-protection framework. The General Data Protection Regulation (GDPR) 2016/679 establishes rights to information, access, and human review of automated decisions (Articles 13–22). The European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) interpret these rights as extensions of dignity and autonomy. In *Digital Rights Ireland v. Minister for Communications* (2014), the CJEU invalidated mass data retention laws for disproportionate interference with privacy [41]. Predictive policing tools that rely on mass data profiling would therefore trigger strict proportionality review.

The proposed **Artificial Intelligence Act (AIA)** further categorizes predictive policing as a *high-risk* application, mandating transparency, risk assessment, and human oversight [20]. Unlike the U.S., where trade-secret law shields algorithmic design, the E.U. demands *explainability by default*. However, practical enforcement remains uneven across Member States, and the tension between security imperatives and fundamental rights persists [42]. The E.U.’s normative framework is thus aspirational but not yet structurally realized.

3.3 Convergence and Divergence

Both jurisdictions grapple with the paradox of algorithmic objectivity: how to preserve individual rights in systems optimized for collective prediction. The U.S. emphasizes pragmatic reasonableness, while the E.U. emphasizes ethical proportionality. Yet convergence appears in emerging calls for algorithmic transparency and accountability audits [43], [44]. The divergence lies in legal philosophy: American constitutionalism presumes liberty against power, whereas European human-rights law presumes dignity within community. Predictive policing tests both premises by embedding power within code.

4. Policy and Doctrinal Reforms

4.1 Algorithmic Impact Assessments (AIA) and Disclosure Duties

Legislatures should mandate *Algorithmic Impact Assessments* analogous to environmental reviews. Before deployment, agencies must disclose training data sources, model architecture, validation metrics, and bias-mitigation strategies. This mirrors the transparency provisions of the E.U. AIA Act and aligns with the NIST AI Risk Management Framework (2023) [45]. Disclosure obligations would reintroduce ex ante accountability, allowing courts and civil-society watchdogs to evaluate predictive models before rights are violated.

4.2 Independent Algorithmic Auditing

Courts should authorize neutral algorithmic auditors—akin to forensic experts—to test model validity and detect disparate impact. Veale and Edwards's model of "adversarial transparency" allows independent evaluation without compromising intellectual property [46]. Judicial accreditation of such auditors would institutionalize algorithmic due process, ensuring that evidence derived from AI meets constitutional reliability standards under *Daubert*.

4.3 Statutory Right to Explanation and Contestability

U.S. due-process doctrine must evolve to include a statutory *Right to Explanation* similar to GDPR Article 22. Individuals subject to algorithmic policing should have access to meaningful information about model logic and decision parameters. Legislative reforms—such as the proposed Algorithmic Accountability Act—should codify this right, ensuring that algorithmic determinations can be challenged in court [47]. Without contestability, due process becomes procedural theater.

4.4 Judicial Re-interpretation of Reasonable Suspicion

Courts must reinterpret *reasonable suspicion* to account for algorithmic mediation. Judicial scrutiny should assess not only the officer's reliance on data but also the data's epistemic integrity. Predictive models should be treated as *expert witnesses* whose methodologies are subject to cross-examination. Failure to disclose algorithmic reasoning should trigger exclusion under the Fourth Amendment's exclusionary rule, preserving constitutional deterrence [48].

4.5 Ethical and Institutional Re-orientation

Law enforcement culture must shift from techno-optimism to constitutional humility. Training programs should integrate algorithmic literacy, emphasizing bias recognition and data ethics. Oversight boards composed of technologists, ethicists, and community representatives can ensure that predictive systems serve public safety without eroding civil rights [49]. Ultimately, accountability must be structural, not discretionary.

Conclusion

The rise of predictive policing marks a constitutional inflection point. The migration from *probable cause* to *predictive cause* replaces judgment with computation, embedding historical bias within the machinery of law enforcement. Algorithmic immutability transforms suspicion into destiny, eroding due process and equal protection while evading judicial scrutiny under the shield of trade secrecy. Comparative analysis reveals that while the European Union articulates stronger normative safeguards, neither jurisdiction has reconciled technological precision with constitutional legitimacy.

To restore this balance, law must reclaim its epistemic sovereignty. Probable cause must remain a human judgment grounded in evidence, not a probability score derived from opaque models. Transparency, contestability, and accountability are not technical luxuries—they are constitutional imperatives. By embedding algorithmic audits, disclosure duties, and rights to explanation within the legal framework, societies can ensure that the predictive state does not eclipse the rule of law. Only then can Artificial Intelligence serve justice without redefining it.

References

[1] A. G. Ferguson, *The Rise of Big Data Policing*, New York University Press, 2017.

[2] S. Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing*, Oxford University Press, 2020.

[3] E. Joh, “Policing by Numbers: Big Data and the Fourth Amendment,” *Wash. L. Rev.*, vol. 89, 2014.

[4] *Terry v. Ohio*, 392 U.S. 1 (1968).

[5] *Illinois v. Gates*, 462 U.S. 213 (1983).

[6] A. Crawford and K. Paglen, “Excavating AI: The Politics of Images in Machine Learning,” *AI & Society*, vol. 35, 2020.

[7] M. Kroll et al., “Accountable Algorithms,” *U. Pa. L. Rev.*, vol. 165, 2017.

[8] D. Citron, “Technological Due Process,” *Wash. U. L. Rev.*, vol. 85, 2008.

[9] A. Selbst and S. Barocas, “The Intuitive Appeal of Explainable Machines,” *Fordham L. Rev.*, vol. 87, 2018.

[10] S. Lum and W. Isaac, “To Predict and Serve?,” *Significance*, vol. 13, 2016.

[11] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, “Machine Bias,” *ProPublica*

Report, 2016.

[12] C. O'Neil, *Weapons of Math Destruction*, Crown, 2016.

[13] M. Hildebrandt, "Law as Computation in the Era of Artificial Legal Intelligence," *Artificial Intelligence and Law*, vol. 25, 2017.

[14] N. Desai and J. Kroll, "Algorithmic Suspicion," *Harv. J. L. & Tech.*, vol. 34, 2021.

[15] A. Raza, "Trade Secrets as a Substitute for AI Protection: A Critical Investigation into Different Dimensions of Trade Secrets," 2024.

[16] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

[17] *Whren v. United States*, 517 U.S. 806 (1996).

[18] *Washington v. Davis*, 426 U.S. 229 (1976).

[19] *Carpenter v. United States*, 585 U.S. ___ (2018).

[20] S. Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, 2019.

[21] I. Hacking, *The Social Construction of What?*, Harvard University Press, 1999.

[22] *United States v. Jones*, 565 U.S. 400 (2012).

[23] N. Wiener, *Cybernetics and Society*, MIT Press, 1954.

[24] E. W. Felten and M. Reed, "Transparency as Accountability," *Yale J. L. & Tech.*, vol. 23, 2021.

[25] P. Veale and L. Edwards, "Clarity, Surprise, and Normativity: Transparency in Algorithmic Systems," *Yale J. L. & Tech.*, vol. 20, 2018.

[26] European Commission, *Proposal for an Artificial Intelligence Act*, COM (2021) 206 final.

[27] National Institute of Standards and Technology, *AI Risk Management Framework 1.0*, 2023.

[28] B. Casey and J. Calo, "Rethinking Police Reliance on Algorithms," *Nw. U. L. Rev.*, vol. 114, 2019.

[29] L. Hannah-Moffat, "Algorithmic Risk and the Re-institutionalization of Inequality," *Theoretical Criminology*, vol. 23, 2019.

[30] C. Heinzelman, "Transparency by Design," *Colum. Sci. & Tech. L. Rev.*, vol. 25, 2023.

[31] R. Calo, "Artificial Intelligence Policy: A Primer and Roadmap," *UCLA L. Rev.*, vol. 51, 2020.

[32] E. K. Crawford and J. D. Paglen, "Excavating AI," *AI & Society*, vol. 35, 2020.

[33] B. Latour, *Reassembling the Social*, Oxford University Press, 2005.

[34] M. Goodman, “Ethical Constraints on Predictive Policing,” *Ethics and Information Technology*, vol. 25, 2023.

[35] E. Shapiro, “Algorithmic Accountability in the Criminal Justice System,” *Brooklyn L. Rev.*, vol. 89, 2024.

[36] H. Shneiderman, *Human-Centered AI*, Oxford University Press, 2022.

[37] M. Pasquale, *The Black Box Society*, Harvard University Press, 2015.

[38

] D. Keats Citron and F. Pasquale, “The Scored Society: Due Process for Automated Predictions,” *Wash. L. Rev.*, vol. 89, 2014.

[39] M. Kearns and A. Roth, *The Ethical Algorithm*, Oxford University Press, 2019.

[40] G. Strahilevitz, “Algorithmic Reasonableness,” *U. Chi. L. Rev.*, vol. 90, 2023.

[41] *Digital Rights Ireland v. Minister for Communications*, C-293/12, EU:C:2014:238.

[42] M. Pizzi, “Transparency in Algorithmic Policing: Lessons from the EU,” *Eur. L. J.*, vol. 28, 2022.

[43] J. E. Cohen, “Between Truth and Power: The Legal Constructions of Informational Capitalism,” Oxford University Press, 2019.

[44] R. Braithwaite, “Regulating Risk Prediction: A Human Rights Approach,” *Human Rights L. Rev.*, vol. 23, 2023.

[45] J. Binns, “Fairness in Machine Learning: EU Perspectives,” *Comput. Law & Security Rev.*, vol. 47, 2022.

[46] P. Nemitz, “Constitutional Democracy and Technology in the Age of AI,” *Philos. Trans. R. Soc. A.*, vol. 376, 2018.

[47] C. Docksey, “Accountability in Data Protection and AI,” *Common Market L. Rev.*, vol. 60, 2023.

[48] J. Redish, “Constitutional Audits of AI,” *Yale L. & Policy Rev.*, vol. 42, 2024.

[49] R. Wexler, “When a Computer Program Keeps You in Jail,” *New York Times*, 2017.