Wisdom Vortex:
International Journal of Social Science and Humanities

Open-access, Peer Reviewed, Refereed, Quarterly Journal, Multiple Language (English & Hindi)

e-ISSN: 3107-3808
p-ISSN: Applied for

Wisdom Vortex: International Journal of Social Science and Humanities, Volume: 02, Issue: 03, Oct-Dec 2026

How to cite this paper:
Mandal, S. (2026). Critical Perspectives on Algorithmic Bias and Due Process in Criminal Adjudication. *Wisdom Vortex: International Journal of Social Science and Humanities, 2*(3), 25-33.
https://doi.org/10.64429/wvijsh.02.03.051

Received: 19 Aug. 2026
Accepted: 25 Sep. 2026
Published: 10 Oct. 2026

Copyright © 2026 by author(s) and Wisdom Vortex: International Journal of Social Science and Humanities.
This work is licensed under the Creative Commons Attribution 4.0 International License (CC BY- 4.0).
https://creativecommons.org/licenses/by/4.0/

Critical Perspectives on Algorithmic Bias and Due Process in Criminal Adjudication

Dr. Subir Mandal[1]

ABSTRACT

The integration of artificial intelligence and algorithmic risk-assessment into criminal adjudication marks a shift from judicial discretion to data-driven governance. Proponents claim these tools eliminate bias and docket delays; however, this review demonstrates that algorithmic models instead institutionalize historical inequities under a veneer of scientific infallibility. By ingesting datasets corrupted by over-policing, machine-learning systems mistake enforcement patterns for objective behavioral forecasts, penalizing marginalized groups through proxy variables and feedback loops. Crucially, this automated turn conflicts with due process and equal protection. When private vendors assert trade-secret privileges to shield source code and feature weights, defendants are denied the right to confront adverse evidence and secure reasoned rulings. Furthermore, automation bias leads judges to defer uncritically to probabilistic classifications, delegating qualitative judicial authority to corporate actors. Synthesizing comparative frameworks across the United States, European Union, and India, this paper argues for constitutional supremacy. It proposes enforceable safeguards, including codified algorithmic discovery rights, mandatory human-in-the-loop limits, pre-deployment impact assessments, and strict exclusionary rules, to ensure technological modernization does not compromise human liberty.

Keywords: *Algorithmic Bias, Due Process, Criminal Adjudication, Risk Assessment Tools, Constitutional Safeguards*

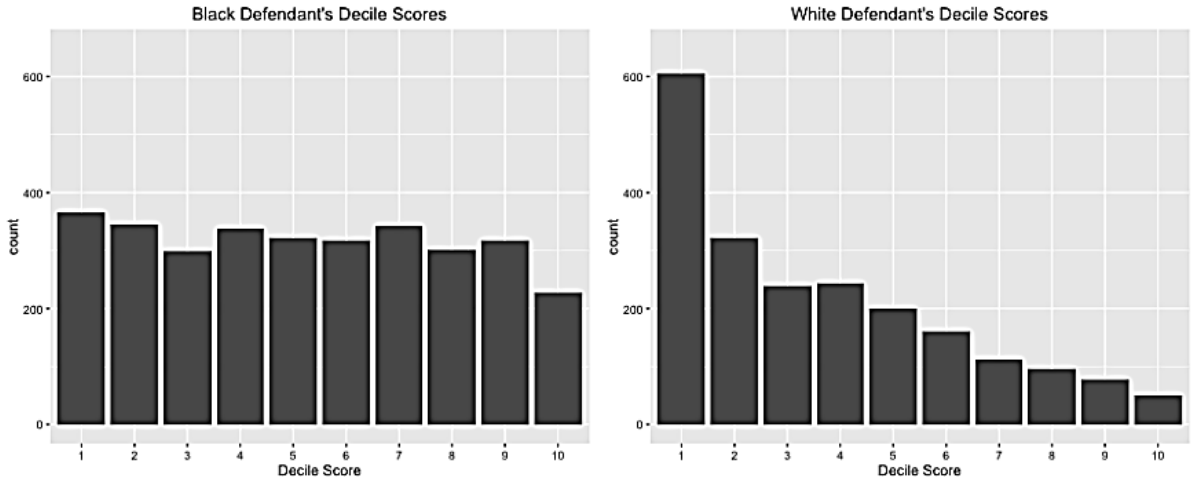
Criminal courtrooms across the world are undergoing a silent revolution. Decisions once left entirely to human discretion such as granting pretrial bail, determining prison sentences, and assessing parole eligibility are now steadily outsourced to artificial intelligence and automated risk-assessment software (Berk, 2012; Ferguson, 2017). These algorithmic systems process historical arrest records,

[1] Assistant Professor, Deptt. of Legal Studies, SNU, Kolkata, WB

demographic proxies, and socio-economic variables to generate a statistical "risk score," estimating the mathematical likelihood that an individual will reoffend (Kehl et al., 2017). On paper, the appeal is undeniable: algorithms do not suffer from mental fatigue, do not exhibit overt personal animus, and can evaluate massive caseloads with administrative efficiency (Kleinberg et al., 2018). However, judicial reality presents a starkly different picture. An algorithm remains only as neutral as the historical data fed into its neural networks. Because modern criminal registries reflect decades of unequal policing, systemic poverty, and selective arrest practices, machine learning models routinely mistake past institutional inequities for objective future predictions (Barocas & Selbst, 2016; Benjamin, 2019). Far from eliminating human prejudice, these automated tools frequently repackage systemic social bias into seemingly impartial, scientific metrics that disproportionately penalize marginalized defendants (Angwin et al., 2016; O'Neil, 2016). This computational shift sparks a profound constitutional crisis: Can an automated adjudication system ever satisfy procedural fairness when shielded behind impenetrable proprietary code? This paper argues that deploying automated risk scores in criminal adjudication fundamentally undermines foundational procedural due process. When private vendors invoke trade-secret protections to conceal their source code, defendants lose the fundamental legal right to inspect, challenge, and cross-examine the evidence deciding their personal liberty (Citron, 2008; Pasquale, 2015). Drawing upon a doctrinal and comparative framework, this review evaluates key statutory instruments and landmark judicial decisions ranging from the evidentiary controversies of State v. Loomis (2016) in the United States, to the European Union AI Act (European Parliament, 2024), and the inviolable fair-procedure mandates under Articles 14 and 21 of the Indian Constitution (Maneka Gandhi, 1978; Puttaswamy, 2017) interrogating where computational convenience ends and constitutional human rights must prevail.

Conceptualizing Algorithmic Bias in Criminal Law

Algorithmic bias in the penal context cannot be understood merely as a technical bug or random computational error. Instead, it constitutes a structural phenomenon where algorithmic models systematically produce outcomes that privilege one demographic group over another (Barocas & Selbst, 2016). When algorithmic tools are integrated into criminal proceedings, mathematical abstractions interact with institutional power structures, converting pre-existing socio-legal inequalities into seemingly objective predictive outputs (Crawford, 2021). To understand this interaction, algorithmic bias must be classified into its core structural components.



Taxonomy of Algorithmic Bias

The propagation of algorithmic bias across criminal adjudication operates through a tightly coupled triadic framework: training data skews, latent proxy discrimination, and systemic feedback loops. Fundamentally, machine learning models depend on historical datasets to project future criminal behavior, but in penal contexts, this data records sovereign enforcement

patterns such as stop-and-frisk incidents, selective arrests, and disparate conviction rates rather than actual underlying criminality (Ferguson, 2017). Because law enforcement practices have historically subjected impoverished, racialized, and socially marginalized groups to disproportionate surveillance, the resulting baseline training sets are inherently skewed; an algorithm trained on decades of arrest registries learns not who commits offenses, but whom the state historically targeted and prosecuted (Benjamin, 2019; Richardson et al., 2019). While system developers routinely omit protected attributes like race, caste, or religion to satisfy formal anti-discrimination mandates, algorithmic architectures readily bypass these omissions through proxy discrimination (Barocas & Selbst, 2016). Non-protected variables such as residential postal codes, parental arrest histories, credit indicators, and employment stability correlate strongly with marginalized social identities due to entrenched structural inequalities, allowing complex models to statistically reconstruct the excluded protected traits and generate discriminatory disparate impact behind a facade of technical neutrality (Kroll et al., 2017; Prince & Schwarcz, 2020). This dynamic culminates in self-fulfilling, runaway feedback loops: when automated tools assign elevated risk profiles to individuals from specific communities, courts deny bail and impose punitive custodial sentences, prompting law enforcement to concentrate surveillance in those exact vicinities (Brayne, 2020; Ensign et al., 2018). The resulting spike in local arrests stemming from heightened scrutiny rather than higher baseline deviance is subsequently fed back into the system as empirical validation, causing the algorithm to validate its own structural biases through recursive learning while shielding flawed predictive assumptions from independent judicial scrutiny (Harcourt, 2007; Lum & Isaac, 2016; O'Neil, 2016).

Key Global and Domestic Benchmarks

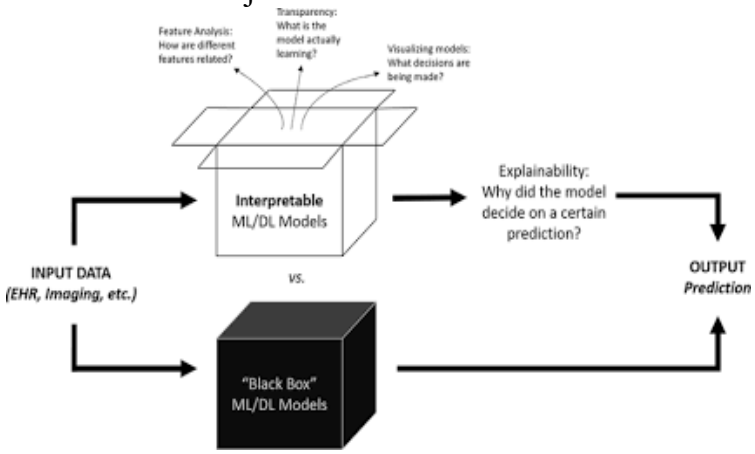
Metric / Benchmark	Operational Target	Empirical Finding	Constitutional / Legal Implication
COMPAS Recidivism Scores *(Broward County, USA)*	Pretrial bail and sentencing risk scoring	Black defendants were falsely labeled high risk at nearly twice the rate of white defendants (44.9% vs. 23.5%) (Angwin et al., 2016).	Violated equal treatment principles; challenged under 14th Amendment Due Process in *State v. Loomis* (2016).
Facial Recognition Tech (FRT) *(e.g., Delhi Police, UK Met Police)*	Suspect identification and automated tracking	Error rates for darker-skinned women reached up to 34.7%, compared to less than 1% for lighter-skinned men (Buolamwini & Gebru, 2018).	False arrests, wrongful detention, and violation of bodily autonomy and privacy (*K.S. Puttaswamy*, 2017).
Automated Case Allocation & Risk Flags *(Judicial CMS Tools)*	Case categorization and scheduling priority	Proprietary prioritization models obscure why certain cases face administrative delays or adverse scrutiny.	Breaches judicial duty to provide reasoned orders and natural justice (*audi alteram partem*).

The real-world manifestation of these mechanisms is illustrated by the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool, evaluated extensively in United States jurisprudence. In State v. Loomis (2016), the Wisconsin Supreme Court addressed a due process challenge against COMPAS, where the defendant argued that reliance on a proprietary, trade-secret algorithm prevented him from assessing the accuracy and scientific validity of the score used against him. While the court permitted the use of COMPAS, it explicitly warned that proprietary scores cannot form the sole determinant of a sentence, acknowledging the tool's demonstrated racial disparities and lack of procedural explainability (Eckhouse et al., 2019; Kehl et al., 2017). Similarly, the deployment of automated facial

recognition technology (FRT) in police investigations such as initiatives by metropolitan police agencies in London and automated surveillance pilots across major Indian urban centers demonstrates significant empirical divergence across demographic lines (Buolamwini & Gebru, 2018; Garvie et al., 2016). Because deep convolutional neural networks are predominantly trained on skewed benchmark image datasets, misidentification rates spike drastically among women and individuals with darker skin tones (Raji et al., 2020). When law enforcement treats probabilistic biometric matches as actionable probable cause, the burden shifts onto the citizen to disprove an unverified machine output, threatening fundamental liberties under Article 21 of the Indian Constitution and Fourth Amendment jurisprudence in the United States (Ferguson, 2017; Joh, 2019).

Due Process in the Age of Automated Decisions

The introduction of algorithmic scoring mechanisms into the criminal justice process forces a direct collision between computational efficiency and constitutional due process. While traditional procedural fairness guarantees an accused the right to understand, interrogate, and refute evidence that affects their liberty, algorithmic adjudication introduces systemic opacity, undermines judicial reasoning, distorts evidentiary burdens, and triggers cognitive cognitive biases in human adjudicators.



- **The "Black-Box" Problem and Procedural Transparency:** At the core of automated decision-making lies the black-box dilemma: the internal mathematical transformations, feature weightings, and source code governing an algorithmic output are inaccessible to outside examination. In criminal proceedings, this technical opacity is reinforced by commercial law. Private software vendors claim proprietary trade-secret privilege over their scoring models, preventing defense attorneys from scrutinizing source code, input weightings, or validation metrics (Pasquale, 2015; Wexler, 2018). This commercial barrier directly infringes upon the defendant's constitutional right to cross-examine evidence. As demonstrated in State v. Loomis (2016), the defendant was denied access to the proprietary methodology of Northpointe's COMPAS tool, forcing the defense to contest a risk metric without knowing which specific variables produced the adverse score. By subordinating criminal discovery rights to private intellectual property claims, the justice system allows state coercion to rely on unauditable computational assertions (Citron, 2008).
- **The Right to a Reasoned Decision and Audi Alteram Partem:** A foundational requirement of natural justice and procedural due process is the duty of judicial officers to deliver reasoned orders. A reasoned order demonstrates that the court engaged with the facts, applied legal rules, and provided the parties an opportunity to be heard (audi alteram partem). Deep machine learning and complex actuarial tools break this chain of accountability because their decision boundaries are fundamentally non-interpretable, even to the developers who design them (Burrell, 2016; Selbst & Barocas, 2018). When a magistrate or sentencing judge relies on a probabilistic score without understanding how distinct input factors generated that outcome, the resulting order fails the legal test of meaningful justification. Instead of articulating substantive judicial logic, the court effectively rubber-stamps an opaque statistical output, reducing the constitutional

guarantee of a fair hearing to an administrative formality (Cobbe, 2019; Hildebrandt, 2016).

- **Evidentiary Integrity and the Presumption of Innocence**: Algorithmic risk assessments disrupt the allocation of evidentiary burdens in criminal proceedings. Under constitutional due process, the state carries the burden of proving culpability beyond a reasonable doubt, and personal liberty can be curtailed only upon clear, individualized evidence. Risk tools, by contrast, operate on group-level statistical generalities: they infer an individual's future conduct based on the historical behavior of a demographic cohort sharing similar characteristics (Harcourt, 2007; Ferguson, 2017). When an algorithm classifies a defendant as "high risk," it constructs an evidentiary presumption of dangerousness. In bail and sentencing determinations, this dynamic effectively shifts the burden of proof onto the accused, who must disprove a future risk score derived from hidden algorithmic assumptions (Mayson, 2019). This transition from adjudicating past deeds to penalizing actuarial profiles compromises the presumption of innocence.
- **Automation Bias in the Judiciary:** Proponents often argue that risk assessment tools function merely as non-binding judicial aids, leaving ultimate discretion with the presiding judge. Cognitive psychology and empirical legal research demonstrate that this human-in-the-loop safeguard is largely illusory due to automation bias the tendency of human decision-makers to defer to automated systems and overlook conflicting qualitative information (Cummings, 2017; Parasuraman & Manzey, 2010). In high-volume court environments marked by crushing caseloads and tight time constraints, judges and magistrates routinely rely on algorithmic scores as an epistemic shortcut (Slobogin, 2014). Deviating downward from a "high risk" algorithmic rating exposes a judge to severe reputational and public backlash if the released individual reoffends, whereas following the machine's warning provides institutional cover. Consequently, probabilistic outputs operate with de facto binding force, displacing nuanced, individualized judicial evaluation in favor of algorithmic consensus (Stevenson, 2018; Garrett & Monahan, 2020).

Constitutional & Jurisprudential Implications

The integration of algorithmic decision-making tools into the penal apparatus directly tests core constitutional doctrines designed to constrain state power and protect individual liberty, colliding sharply with equal protection guarantees, procedural fairness mandates, and the non-delegation of judicial authority. While classical equal protection standards under the Fourteenth Amendment of the United States Constitution and Article 14 of the Constitution of India historically required proving purposeful, discriminatory intent (Washington v. Davis, 1976), automated risk assessment instruments generate profound systemic inequities through statistical proxies (Barocas & Selbst, 2016). By converting neutral variables such as residential zip codes, employment histories, and familial arrest records into predictive markers of dangerousness, algorithmic models reproduce historical patterns of marginalization behind a facade of scientific objectivity. Contemporary constitutional jurisprudence in India explicitly proscribes such indirect discrimination and manifest arbitrariness (Lt. Col. Nitisha, 2021; Shayara Bano, 2017), rendering opaque algorithmic classifications vulnerable to constitutional invalidation for lacking an intelligible differentia and a rational nexus to legitimate penological goals.

Concurrently, procedural due process dictates that any state deprivation of liberty must satisfy rigorous fairness requirements. Under Article 21 of the Indian Constitution, procedure established by law must be just, fair, and reasonable (Maneka Gandhi, 1978). By shielding underlying source code, optimization weights, and predictive variables behind commercial trade-secret protections, proprietary tools deny defendants the fundamental right to inspect, challenge, and cross-examine adverse evidence (Citron, 2008). This structural opacity violates the procedural guarantee of audi alteram partem and fails the constitutional proportionality

standard enunciated in K.S. Puttaswamy (2017), replacing individualized evidentiary assessment with probabilistic cohort generalities. Beyond individual rights, algorithmic governance causes an impermissible delegation of core judicial authority. Although framed as advisory aids, institutional docket pressures and cognitive automation bias induce judges to defer routinely to actuarial scores, impermissibly fettering lawful judicial discretion (Wednesbury Corp., 1948). This dynamic effectively outsources qualitative fact-finding to unaccountable commercial software vendors, transforming constitutional adjudication into unreviewable computational determinism (Pasquale, 2015).

Critical Review of Existing Regulatory Frameworks

Existing regulatory models exhibit profound cross-jurisdictional divergence in addressing the rapid proliferation of algorithmic tools within penal systems. The European Union has established the world's most comprehensive risk-based regime under the EU Artificial Intelligence Act (European Parliament, 2024). This framework explicitly categorizes artificial intelligence systems deployed by judicial authorities and law enforcement agencies specifically tools utilized for individual risk assessment, recidivism forecasting, and evidence evaluation as "high-risk" applications. Under this statutory designation, developers and deploying judicial bodies must comply with strict conformity assessments, mandatory data governance standards, comprehensive technical logging, and meaningful human oversight mechanisms before deployment. Conversely, the regulatory landscape in the United States remains highly decentralized, relying on a fragmented patchwork of state-level algorithmic accountability bills, disparate administrative guidelines, and traditional criminal discovery rules. Rather than establishing comprehensive ex-ante oversight, American courts predominantly evaluate automated instruments ex-post through constitutional challenges. However, this approach routinely falters because evidentiary disclosure standards frequently subordinate a criminal defendant's sixth amendment and due process rights to the commercial trade-secret protections claimed by private software vendors (Wexler, 2018). As private intellectual property privileges continue to shield proprietary scoring models, criminal defense counsel is systematically prevented from conducting independent source-code audits or cross-examining adverse algorithmic assertions in open court.

India occupies a distinct position marked by an acute statutory vacuum concerning public-sector algorithmic governance. While the Digital Personal Data Protection Act establishes a baseline framework for commercial and personal data processing, it grants sweeping sovereign exemptions to state security agencies and law enforcement bodies. Consequently, predictive policing software, facial recognition deployments, and emergent judicial automation pilots operate without comprehensive statutory boundaries, public algorithmic impact registries, or mandatory explainability mandates. Compounding these regulatory shortcomings is an institutional over-reliance on voluntary corporate self-regulation and superficial technical interventions. Developers frequently claim that mathematical debiasing techniques, demographic parity recalibrations, and post-hoc feature explanations can resolve constitutional inequities. Yet, technical fixes remain structurally inadequate because mathematical adjustments cannot neutralize historical over-policing or systemic socioeconomic marginalization reflected in underlying state data (Barocas & Selbst, 2016). Mere statistical balancing cannot cure the fundamental denial of due process when an individual's liberty remains subject to automated, unreviewable carceral instruments.

Proposed Framework: Safeguards & The Path Forward

Reconciling artificial intelligence with criminal justice requires shifting away from voluntary corporate ethics toward enforceable constitutional and statutory safeguards. If automated systems are to exist within judicial administration, they must operate under strict legal constraints that preserve individual liberty, evidentiary transparency, and judicial accountability. To secure procedural due process against computational arbitrariness, legal frameworks must institutionalize four foundational pillars:

- **Statutory Rights to Algorithmic Discovery and Explainability:** Procedural due process demands that no person suffer an adverse judicial determination grounded in evidence they cannot inspect, necessitating an affirmative statutory right to algorithmic discovery in criminal proceedings (Citron, 2008). In matters affecting personal liberty, private intellectual property claims must yield to constitutional fair-trial rights by abrogating trade-secret privileges, ensuring that proprietary source code, training datasets, feature weightings, and error-rate margins are disclosed to defense counsel under appropriate protective orders (Wexler, 2018). Furthermore, system developers must provide contextual explainability through counterfactual and feature-attribution models, ensuring that machine outputs do not arrive as isolated numeric scores, but clearly demonstrate which specific factors produced an adverse risk designation.
- **Enforceable "Human-in-the-Loop" Mandates and Discretionary Primacy:** Automated predictions must never displace the constitutional mandate of individualized judicial reasoning or allow institutional automation bias to compromise judicial independence (Garrett & Monahan, 2020). Statutes must explicitly establish that algorithmic risk scores remain strictly advisory, barring them from functioning as mandatory sentencing baselines or presumptive grounds for bail denial. When a judge consults an automated tool, they must record explicit written reasons showing how independent, qualitative facts justify the final order, ensuring that statistical cohort calculations do not replace the court's constitutional duty to deliver a reasoned judgment (audi alteram partem).
- **Pre-Deployment Algorithmic Impact Assessments (AIAs):** Before any predictive or risk-scoring software is procured or integrated into court administration, it must undergo rigorous Algorithmic Impact Assessments conducted by independent oversight bodies comprising judicial officers, legal scholars, and civil liberties experts. These evaluations must audit baseline data lineage to uncover historical over-policing, sampling disparities, and latent proxy variables that correlate with marginalized castes, races, or socioeconomic backgrounds (Barocas & Selbst, 2016). Furthermore, algorithmic instruments must empirically demonstrate demographic parity and low false-positive error rates prior to procurement, coupled with recurring post-deployment audits to identify and halt compounding feedback loops in live court environments.
- **Judicial Exclusionary Rules for Unaudited and Proprietary Systems:** The ultimate safeguard against computational arbitrariness lies in robust judicial gatekeeping through an unyielding exclusionary rule. Courts must deem inadmissible any algorithmic output derived from systems that have not been independently audited, publicly registered, and subjected to rigorous defense cross-examination. If a commercial software vendor asserts trade-secret privilege to withhold source code, methodological parameters, or validation audits from open court proceedings, the resulting risk score must be excluded entirely from bail determinations, sentencing memorandums, and parole reviews, preserving constitutional legitimacy over administrative convenience.

CONCLUSION

The integration of artificial intelligence and algorithmic risk-assessment instruments into criminal adjudication represents a profound transformation in how the state exercises carceral power. Proponents have long advanced computational automation as a transformative solution to human inconsistency, cognitive exhaustion, and systemic case backlogs, promising an era of objective, data-driven equity. However, this critical review demonstrates that algorithmic models do not eliminate systemic disparities; rather, they formalize, accelerate, and obscure them under an unearned veneer of scientific infallibility. By drawing upon training datasets poisoned by decades of selective enforcement and over-policing, algorithmic systems mistake historical state bias for empirical truth. Through proxy variables and recursive feedback loops, automated tools disproportionately penalize marginalized demographics while shielding

structural discrimination behind complex mathematical models. This dynamic poses an irreconcilable conflict with constitutional guarantees of due process, procedural fairness, and the equal protection of laws. When private commercial vendors invoke trade-secret protections to conceal source code, validation statistics, and weighting metrics, the criminal defendant is effectively stripped of the foundational right to confront adverse evidence and demand a reasoned judicial determination. Furthermore, cognitive automation bias induces judicial officers to defer uncritically to probabilistic cohort classifications, creating an unlawful delegation of qualitative judicial discretion to unaccountable software developers. The path forward does not require a Luddite rejection of technological innovation, but an uncompromising reassertion of constitutional primacy. While administrative modernization can assist court infrastructure and case docket management, algorithmic instruments must never be allowed to dictate substantive questions of human liberty, guilt, or punishment. Judicial systems must institutionalize strict statutory rights to algorithmic discovery, enforce genuine human-in-the-loop oversight, mandate independent pre-deployment impact assessments, and apply uncompromising exclusionary rules against unaudited proprietary systems. Ultimately, procedural due process exists precisely to protect individuals from sovereign convenience. A criminal justice system that trades transparency, natural justice, and the presumption of innocence for administrative speed surrenders its moral authority, transforming the constitutional promise of fair adjudication into unreviewable computational determinism.

REFERENCES

Allen, T. D., Golden, T. D., & Shockley, K. M. (2015). How effective is telecommuting? Assessing the status of our scientific findings. *Psychological Science in the Public Interest*, 16(2), 40–68. https://doi.org/10.1177/1529100615593273

Allen, T. D., Herst, D. E., Bruck, C. S., & Sutton, M. (2015). Consequences associated with work-to-family conflict: A review and agenda for future research. *Journal of Occupational Health Psychology*, 5(2), 278–308. https://doi.org/10.1037/1076-8998.5.2.278

Ashforth, B. E. (1997). Petty tyranny in organizations: A preliminary examination of antecedents and consequences. *Human Relations*, 50(7), 755–778.

Bakker, A. B., & Demerouti, E. (2017). Job demands–resources theory: Taking stock and looking forward. *Journal of Occupational Health Psychology*, 22(3), 273–285. https://doi.org/10.1037/ocp0000056

Bowling, N. A., & Beehr, T. A. (2006). Workplace harassment from the victim's perspective: A theoretical model and meta-analysis. *Journal of Applied Psychology*, 91(5), 998–1012. https://doi.org/10.1037/0021-9010.91.5.998

Cropanzano, R., Anthony, E. L., Daniels, S. R., & Hall, A. V. (2017). Social exchange theory: A critical review with theoretical remedies. *Academy of Management Annals*, 11(1), 479–516. https://doi.org/10.5465/annals.2015.0099

Detert, J. R., & Edmondson, A. C. (2011). Implicit voice theories: Taken-for-granted rules of thumb that inhibit employee voice. *Academy of Management Journal*, 54(3), 461–488. https://doi.org/10.5465/amj.2011.61967910

Edmondson, A. C., & Lei, Z. (2014). Psychological safety: The history, renaissance, and future of an interpersonal construct. *Annual Review of Organizational Psychology and Organizational Behavior*, 1(1), 23–43. https://doi.org/10.1146/annurev-orgpsych-031413-091305

Einarsen, S., Aasland, M. S., & Skogstad, A. (2007). Destructive leadership behaviour: A definitions and conceptual model. *The Leadership Quarterly*, 18(3), 207–216.

Galanti, T., Guidetti, G., Mazzei, E., Zappalà, S., & Toscano, F. (2021). Work from home during the COVID-19 outbreak: The impact on employees' remote working distress, engagement, stress, and exhaustion. *Journal of Occupational and Environmental Medicine*, 63(7), e426–e432. https://doi.org/10.1097/JOM.0000000000002236

Halbesleben, J. R. B., Neveu, J.-P., Paustian-Underdahl, S. C., & Westman, M. (2014). Getting to the "COR": Understanding the role of resources in conservation of resources theory. *Journal of Management*, 40(5), 1334–1364. https://doi.org/10.1177/0149206314527130

Harter, J. K., et al. (2020). Well-being at work and its relationships with business outcomes: A multi-company, multi-level study. *Journal of Applied Psychology*, 105(8), 841–862.

Hobfoll, S. E. (2001). The influence of culture, community, and the nested-self in the stress process: Advancing conservation of resources theory. *Applied Psychology: An International Review*, 50(3), 337–421. https://doi.org/10.1111/1464-0597.00062

Inceoglu, I., Thomas, G., Chu, C., Plans, D., & Gerbasi, A. (2018). Leadership behavior and employee well-being: An integrated review and a future research agenda. *The Leadership Quarterly*, 29(1), 179–202. https://doi.org/10.1016/j.leaqua.2017.12.006

Karlsson, J., et al. (2021). Dark triad leadership and employee outcomes: A systematic review. *Leadership & Organization Development Journal*, 42(5), 712–730.

Kelloway, E. K., Turner, N., Barling, J., & Loughlin, C. (2012). Transformational leadership and employee psychological well-being: The mediating role of employee trust in leadership. *Work & Stress*, 26(1), 39–55. https://doi.org/10.1080/02678373.2012.660774

Mackey, J. D., Frieder, R. E., Brees, J. R., & Martinko, M. J. (2017). Abusive supervision: A meta-analysis and empirical review. *Journal of Management*, 43(6), 1940–1965. https://doi.org/10.1177/0149206315573997

Maslach, C., Schaufeli, W. B., & Leiter, M. P. (2001). Job burnout. *Annual Review of Psychology*, 52(1), 397–422. https://doi.org/10.1146/annurev.psych.52.1.397

Schyns, B., & Schilling, J. (2013). How bad are the effects of bad leaders? A meta-analysis of destructive leadership and its consequences. *The Leadership Quarterly*, 24(1), 138–158. https://doi.org/10.1016/j.leaqua.2012.09.004

Tepper, B. J. (2000). Consequences of abusive supervision. *Academy of Management Journal*, 43(2), 178–190.

Tepper, B. J. (2007). Abusive supervision in work organizations: Review, synthesis, and research agenda. *Journal of Management*, 33(3), 261–289. https://doi.org/10.1177/0149206307300812