JOURNAL OF CRIMINOLOGY AND CRIMINAL JUSTICE

Vol.2, No.1 2026 E-ISSN. 3137-0543. P-ISSN. 3137-0535 OPEN ACCESS

RESEARCH ARTICLE // DOUBLE-BLIND PEER REVIEWED

Artificial Intelligence and the Transformation of Legal Decision-Making

Usama Ahmad Khan[1] **Tara Davenport**[2]

[1] Master's Law of International Trade and Dispute Resolution, School of International Law, Higher School of Economics, Moscow, Russia. Email: ukhan@edu.hse.ru

[2] Centre for International Law at the National University of Singapore. Email: t.davenport711@gmail.com

ABSTRACT

Artificial intelligence is increasingly used to support legal and public decision-making, including legal research, document review, risk assessment, administrative processing, and other forms of decision support. Its use can improve speed, consistency, and institutional capacity, but it can also create risks concerning opacity, discriminatory effects, automation bias, procedural fairness, privacy, and the allocation of responsibility. This article examines those risks through qualitative doctrinal analysis and focused comparative policy analysis. It considers the Wisconsin Supreme Court's decision in State v. Loomis, the European Union Artificial Intelligence Act, Canada's Directive on Automated Decision-Making, Council of Europe guidance on AI and judicial systems, and selected interdisciplinary scholarship. The article argues that the central legal problem is not simply whether an AI system is accurate, but whether its use can be reconciled with requirements of lawful authority, reasoned decision-making, equality, contestability, institutional accountability, and effective remedy. The article further distinguishes decision-support systems from systems that materially automate or determine legal outcomes and argues that the required safeguards should be proportionate to the legal stakes and degree of automation. The analysis also considers Pakistan, where constitutional fair-trial, equality, dignity, and due-process principles provide an existing legal vocabulary for evaluating public-sector AI, while the National Artificial Intelligence Policy 2025 provides a policy framework rather than a substitute for legislation. The article concludes that responsible public-sector AI requires layered governance: lawful authority, impact assessment, procurement controls, validation and monitoring, meaningful human review, reasons and notice, auditability, access to remedy, and institutional technical capacity.

01 ARTICLE HISTORY

Received 11-06-2026
Accepted 01-10-2026
Published 10-10-2026

02 KEYWORDS

Artificial intelligence; legal decision-making; algorithmic governance; automated decision-making; due process; rule of law; algorithmic bias; public-sector AI; AI regulation; Pakistan

03 CORRESPONDING AUTHOR

Usama Ahmad Khan
ukhan@edu.hse.ru

CC BY-NC 4.0 © 2026 The Author(s). Published by JuriSocial Research Center Private Limited. This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International Licence (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.68740/jjccj21

1. Introduction

Artificial intelligence is changing the institutional environment in which legal and administrative decisions are made. Courts, prosecutors, police agencies, regulators and public administrators can use algorithmic systems for tasks ranging from document classification and legal research to risk assessment, fraud detection and case triage. The relevant legal question is therefore no longer whether technology will enter legal decision-making, but under what legal and institutional conditions it may legitimately do so.

The attraction is understandable. Courts and administrative bodies face large caseloads, limited resources and demands for timely decisions. Decision-support systems can process large quantities of information rapidly and can make certain forms of statistical prediction more consistent. These potential benefits, however, do not establish that an algorithmic output is legally sufficient. A legal decision differs from a prediction because it affects rights and interests through an exercise of public authority. The legitimacy of that exercise depends on legal authorization, relevant considerations, reasons, procedural safeguards, and avenues for challenge.

AI therefore changes more than the technical means by which information is processed. It can redistribute practical discretion among judges or officials, software designers, data providers, procurement officers, vendors and institutional policies. A system may formally leave the final decision to a human official while making the algorithmic recommendation difficult to depart from in practice. This creates a governance problem that cannot be solved merely by stating that a human remains "in the loop."

The central research problem addressed by this article is how legal systems should preserve legality, procedural fairness, equality and accountability when AI systems materially influence decisions affecting liberty, property, benefits, immigration status, policing, or access to justice. The article does not assume that AI is inherently unlawful or inherently beneficial. Instead, it examines the conditions under which its use can be reconciled with established legal principles.

The article asks four questions. First, how is AI changing legal and administrative decision-making, and how should decision support be distinguished from decision automation? Second, what legal problems arise concerning due process, equality, transparency, reasons, accountability and individualized judgment? Third, what regulatory and institutional mechanisms are emerging internationally, and what are their limits? Fourth, what implications follow for Pakistan's constitutional and public-administration framework?

The article makes three related contributions. First, it treats AI governance as an administrative-law and rule-of-law problem rather than only a technology-policy problem. Second, it proposes a layered accountability model connecting legal authority, procurement, system validation, human review, reasons, auditability and remedies. Third, it uses Pakistan as a focused domestic context, while avoiding the unsupported assumption that foreign regulatory models automatically apply to Pakistani institutions.

2. Research Questions, Objectives, Scope and Contribution

2.1 Research Questions

- How does AI-assisted and automated decision-making alter the exercise of legal and administrative discretion?
- What challenges do AI systems create for due process, equality, transparency, reason-giving, individualized consideration and accountability?
- How do emerging regulatory frameworks address those challenges, and what institutional safeguards appear transferable across jurisdictions?
- What legal and policy principles should guide the use of consequential AI systems in Pakistan?

2.2 Research Objectives

- To distinguish AI used as decision support from AI used to automate or materially determine legal outcomes.
- To analyze the principal doctrinal challenges created by AI-assisted decision-making.
- To compare selected regulatory and institutional responses, with particular attention to the EU, Canada and judicial-sector guidance.
- To formulate a rights-compatible governance model for consequential public-sector AI and assess its relevance to Pakistan.

2.3 Scope and Limitations

The article focuses on consequential public-sector and legal decision-making rather than AI generally. It does not attempt to review every application of AI in legal practice. Its principal materials are legislation and regulatory instruments, judicial decisions, official policy documents, and established academic scholarship. The article is doctrinal and normative, not empirical: it does not independently test algorithmic accuracy, calculate disparate-impact statistics, or conduct interviews with judges, prosecutors, administrators or vendors. Claims about actual deployment should therefore be understood as claims supported by identified sources, not as an original empirical survey.

3. Literature Review and Research Gap

The literature can be grouped into four overlapping bodies. The first concerns machine learning and law, including the distinction between rule-based expert systems and statistical prediction (Surden, 2014; Lehr & Ohm, 2017). The second examines algorithmic discrimination and fairness, including the difficulty of reconciling competing mathematical definitions of fairness (Barocas & Selbst, 2016; Chouldechova, 2017; Kleinberg et al., 2016). The third concerns opacity, explanation and technological due process (Citron, 2008; Pasquale, 2015; Selbst & Barocas, 2018). The fourth concerns administrative automation and the rule of law, including the implications of automated government decision-making for reasons, review and institutional responsibility (Coglianese & Lehr, 2017; Zalnieriute et al., 2019).

The literature also shows that technical accuracy cannot resolve the normative question of legal fairness. A predictive system can be statistically accurate while still being unsuitable for a particular legal purpose. Conversely, an explainable model can still produce legally objectionable outcomes if the underlying data, legal authority or decision process is discriminatory. NIST's AI Risk Management Framework illustrates this broader socio-technical approach by identifying reliability, safety, security, accountability, transparency, explainability, privacy and fairness as context-dependent trustworthiness characteristics (Tabassi, 2023).

The research gap addressed here is therefore institutional. Much of the literature analyzes individual problems—bias, opacity, explanation, responsibility or administrative automation. This article connects them through the legal decision chain: authority to deploy, procurement, data and validation, operational use, human review, reasons, recordkeeping, audit, and remedy. The contribution is not to claim that these issues have never been studied, but to show how their interaction changes the legal analysis of AI-assisted public decisions.

4. Methodology

This article employs qualitative doctrinal legal research combined with focused comparative policy analysis. Primary legal materials are analyzed first, including judicial decisions and binding or official regulatory instruments. Secondary scholarship is used to identify competing interpretations and theoretical debates. Policy documents are treated as policy or soft-law material unless their legal status provides otherwise.

The comparative analysis uses the European Union, Canada and selected judicial-sector standards as functional comparators. The comparison focuses on six variables: legal basis and scope; risk classification; impact assessment and validation; transparency and reasons; human oversight and contestability; and institutional accountability. Pakistan is examined separately as a domestic application context rather than as a jurisdiction assumed to share the constitutional or institutional structure of the comparators.

The method has two limitations. First, the article cannot establish the actual frequency or accuracy of AI use across all courts and public agencies without empirical data. Second, comparative transferability is constrained by differences in constitutional structure, administrative law, procurement systems and institutional capacity. The recommendations are therefore normative proposals informed by verified legal and policy materials, not claims that a single regulatory model is universally optimal.

5. AI Applications and the Degree of Automation

5.1 Decision Support

AI can assist legal professionals without determining the legal outcome. Examples include document classification, legal research, case-law retrieval, transcription, summarization and predictive analytics used as one input among several. Even here, risks arise if users misunderstand the limits of the system, if outputs are not verified, or if automation bias causes officials to treat recommendations as presumptively correct.

5.2 Risk Assessment and Predictive Policing

Risk-assessment systems can be used in bail, sentencing, parole and other criminal-justice contexts. Predictive-policing systems can be used to allocate resources or identify patterns of suspected criminal activity. These applications raise distinct legal questions because historical criminal-justice data may reflect earlier enforcement patterns. The legal problem is not simply that historical data are imperfect; it is that using those data in decisions about individuals may reproduce or amplify institutional patterns that themselves require legal scrutiny.

5.3 Automated Administrative Decision-Making

Administrative automation can affect benefits, immigration, licensing, fraud detection and other public services. Canada's Directive on Automated Decision-Making is a useful comparator because it applies to automated decision systems used to make administrative decisions or related assessments and requires an Algorithmic Impact Assessment before production, with publication and updating requirements. It also contains transparency and explanation requirements. These are institutional controls rather than a claim that every automated decision is unlawful.

5.4 Generative AI and Legal Practice

Generative AI introduces a related but distinct risk: systems may generate plausible but false legal authorities, quotations or factual propositions. The resulting risk is primarily one of professional verification, competence and procedural reliability. A lawyer or public official cannot transfer the legal responsibility for a filing or decision to the model that produced it. The article therefore treats generative AI as a decision-support technology requiring verification rather than as an autonomous legal authority.

6. Legal Challenges

6.1 Lawful Authority and Due Process

The first question is whether the institution has lawful authority to use an AI system for the relevant decision. A general statutory power to administer a program does not necessarily resolve whether a materially automated method is authorized, particularly where the method affects legal rights or

introduces a new form of classification. The answer depends on the governing constitutional and statutory framework of the jurisdiction.

Due process also requires attention to notice, opportunity to contest relevant information, and the ability to challenge the basis of an adverse decision. The precise content varies by jurisdiction. Accordingly, this article does not posit a universal freestanding "right to an explanation" for every algorithmic output. Rather, it argues that where legal systems already require reasons, notice or effective review, the use of AI cannot be allowed to make those safeguards practically meaningless.

6.2 State v. Loomis and Algorithmic Risk Assessment

State v. Loomis, 881 N.W.2d 749 (Wis. 2016), is an important but frequently overstated authority. The Wisconsin Supreme Court did not prohibit the use of COMPAS. It upheld its use subject to limitations and cautions concerning how the assessment could be used. The case therefore demonstrates a narrower proposition: proprietary risk assessment can coexist with sentencing only within legal constraints, and courts must remain attentive to the limits of the information and the defendant's ability to challenge its use. It should not be presented as establishing a universal constitutional rule for algorithmic sentencing.

6.3 Equality and Algorithmic Bias

Algorithmic discrimination may arise from explicit protected characteristics, proxy variables, historical data, model design, deployment context, or institutional use. The fairness literature demonstrates that different statistical criteria can conflict. This means that technical fairness cannot be defined without a normative decision about which interests the legal system is protecting. Legal analysis should therefore identify the relevant equality rule, protected group, comparator or impact standard, justification framework, and remedy rather than treating "bias" as a self-proving legal conclusion.

6.4 Transparency, Explainability and Reasons

"Black box" should not be treated as a single technical condition. Opacity may result from model complexity, proprietary restrictions, inadequate documentation, poor institutional recordkeeping, or the inability of a post-hoc explanation to reproduce the actual basis of an output. Legal transparency should therefore be decomposed into at least four questions: what system was used; what role it played; what information materially affected the decision; and what reasons the lawful decision-maker adopted. These questions are more legally useful than demanding complete disclosure of source code in every case.

6.5 Automation Bias and Meaningful Human Review

A formal human decision-maker does not necessarily guarantee meaningful human judgment. Automation bias can cause officials to defer to system outputs, particularly where caseloads and time pressures are high. The appropriate legal safeguard is therefore not merely to require a human signature. Institutions should ensure that the official has sufficient authority, time, information and training to reject an algorithmic recommendation and must provide reasons for the final decision where the governing law requires them.

6.6 Accountability, Procurement and the Responsibility Gap

AI accountability is distributed across the public body that selects the system, procurement officials, vendors, data providers, system operators and the official making the final decision. The public body cannot avoid public-law duties merely because a vendor supplies the technology. Procurement contracts should therefore address audit rights, documentation, testing, incident reporting, data governance, version control, security, interoperability, vendor access, and exit arrangements. Trade-secret claims may require protection, but they should not automatically defeat every legally required disclosure or judicial review.

6.7 Privacy, Data Governance and Cybersecurity

AI systems often depend on extensive datasets. Public-sector use therefore raises questions of lawful collection, purpose limitation, data quality, retention, security and access. These issues should be analyzed under the data-protection and constitutional law applicable in the jurisdiction rather than through a generic assertion that AI threatens privacy. Security is equally important: a system used to make or support public decisions must be protected against unauthorized access, manipulation and operational failure.

6.8 The Rule of Law and the Nature of Legal Reasoning

Machine learning is generally predictive and statistical, whereas legal reasoning also involves interpretation, justification, precedent and normative judgment. This difference does not mean that AI can never assist legal reasoning. It means that statistical prediction should not silently replace the legal task of explaining why a particular legal rule applies to a particular person. The strongest rule-of-law concern therefore arises when prediction is treated as if it were legal justification.

7. Comparative Regulatory and Institutional Responses

7.1 European Union

Regulation (EU) 2024/1689 establishes a risk-based framework. Annex III identifies specified high-risk uses, including certain systems used in law enforcement, migration and asylum, essential public services, and administration of justice. Importantly, the Act does not classify every AI system used by a public authority as high-risk; classification depends on the Regulation's definitions and categories. The current consolidated text should be used when citing the Act because its application timetable has been amended. As of September 2026, the Regulation generally applies from 2 August 2026, while some provisions and high-risk obligations have later application dates, including Annex III high-risk obligations scheduled under the current Article 113 timetable.

The EU model is significant because it combines risk classification with obligations concerning governance, documentation, human oversight, accuracy, cybersecurity and transparency. Its legal architecture is more precise than a generic claim that the EU simply "bans high-risk AI." The relevant legal question is which category applies, who has which obligation, and when that obligation becomes applicable.

7.2 United States

The United States does not provide a single comprehensive federal AI statute equivalent to the EU AI Act. Governance is distributed across constitutional doctrine, federal statutes, agency action, procurement requirements, state law and litigation. State v. Loomis illustrates how existing legal doctrine can address AI-assisted sentencing without a dedicated AI statute. The article should not, however, describe the entire U.S. system as uniformly "fragmented" without specifying the federal, state or sectoral context under discussion.

7.3 Canada

Canada provides a particularly useful administrative-law comparator. The Treasury Board Directive on Automated Decision-Making applies to automated decision systems used for administrative decisions or related assessments. It requires an Algorithmic Impact Assessment before production and requires the assessment to be reviewed and updated when system functionality or scope changes. The Directive also contains notice and explanation requirements. This is a concrete example of ex ante administrative governance rather than purely ex post litigation.

7.4 Council of Europe and Judicial AI

The Council of Europe's CEPEJ adopted its European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems in 2018. The Charter emphasizes fundamental rights, non-discrimination, quality and

security, transparency, explainability, and user control. It is not an EU regulation and should not be presented as binding legislation. Its value for this article is institutional: it shows how judicial AI can be governed through principles directed specifically at justice systems.

8. Pakistan: Constitutional and Policy Context

Pakistan does not yet have a comprehensive AI statute equivalent to the EU AI Act. Nevertheless, its constitutional framework provides several legal principles relevant to AI-assisted public decision-making. Article 10A recognizes the right to a fair trial and due process; Article 25 establishes equality before law and equal protection of law; Article 14 protects dignity and the privacy of home; and Article 4 guarantees treatment in accordance with law. These provisions provide a constitutional vocabulary for evaluating automated public decisions, although their precise application will depend on the facts, statutory authority and judicial doctrine in the particular case.

Pakistan's National Artificial Intelligence Policy 2025 is an important policy development. The official policy describes responsible and ethical AI use as a national objective and links AI governance to digitalization, data and the Digital Nation Pakistan Act. The policy is, however, a policy instrument rather than a substitute for an enacted comprehensive AI statute. The distinction matters: recommendations in this article concerning statutory notice, audit, impact assessment or enforceable rights should be understood as proposed legal reforms unless an existing Pakistani law already supplies the relevant duty.

For Pakistan, a particularly important research agenda concerns public procurement and administrative decision-making. If government departments procure AI systems for welfare, taxation, policing, licensing, regulatory inspection or other consequential functions, procurement documents should address auditability, data governance, system validation, security, version control, vendor cooperation and the ability of an affected person or court to obtain sufficient information for meaningful review. This is an area where AI governance can be developed through administrative law and procurement reform even before comprehensive AI legislation is enacted.

9. Integrated Discussion: A Layered Accountability Model

The preceding analysis supports a layered model of AI accountability. The first layer is legal authority: the institution must identify the statutory or constitutional basis for using the system. The second is procurement and design: the public body must acquire a system capable of meeting legal requirements. The third is validation: accuracy, bias, security and context-specific performance must be tested before deployment. The fourth is operational oversight: officials must understand the system's limits and retain genuine authority to reject its output. The fifth is procedural protection: affected persons require whatever notice, reasons, hearing and review rights the governing law provides. The sixth is audit and monitoring: systems require continuing review because data, populations, models and operational conditions change. The seventh is remedy: a person harmed by an AI-assisted decision must have a legally meaningful route to challenge the decision and obtain appropriate relief.

This model also clarifies why a purely technical solution is inadequate. Explainability cannot substitute for lawful authority; accuracy cannot substitute for equality; human oversight cannot substitute for reasons; and an impact assessment cannot substitute for an effective remedy. Conversely, litigation alone may arrive too late to correct systemic procurement or design defects. Effective governance therefore requires ex ante and ex post mechanisms operating together.

10. Recommendations

10.1 Require Algorithmic Impact Assessment for Consequential Public AI

Public authorities should conduct and document risk assessment before deploying AI systems that materially affect legal rights, benefits, liberty, immigration status, policing or other high-impact interests. The assessment should identify purpose, legal authority, data sources, foreseeable risks, validation methods, human oversight, security and available remedies. The exact legal status and publication requirements should be established by statute or binding administrative rules.

10.2 Establish Notice, Reasons and Contestability

Where AI materially contributes to a consequential public decision, the governing framework should provide appropriate notice and sufficient explanation to allow the affected person to understand the role of the system and challenge relevant facts or reasoning. This does not necessarily require disclosure of source code.

10.3 Preserve Meaningful Human Review

Human review should be substantive rather than ceremonial. Officials should have authority, time, information and training to depart from AI recommendations, and institutions should monitor override patterns and workload conditions that may encourage automation bias.

10.4 Reform Public Procurement

AI procurement should require documentation, audit rights, validation access, incident reporting, version control, security obligations, data governance, interoperability and appropriate exit rights. Contracts should not make the government incapable of explaining or defending decisions made with the system.

10.5 Create Independent Technical and Legal Oversight

High-impact public AI should be subject to multidisciplinary oversight combining legal, technical, data-protection and operational expertise. The oversight function should have sufficient independence and authority to suspend or require remediation of systems that fail applicable standards.

10.6 Require Continuing Monitoring

Validation should not be a one-time event. Institutions should monitor performance, data drift, disparate impacts, security incidents and changes in system functionality throughout deployment.

10.7 Protect Administrative Records

The public body should preserve the relevant version of the model or system, material inputs, outputs, human interventions, system documentation and reasons needed to reconstruct a decision. Recordkeeping is essential to judicial and administrative review.

10.8 Develop Pakistan-Specific Rules

Pakistan should consider statutory or binding administrative rules addressing impact assessment, notice, human review, procurement, audit, recordkeeping and remedies for consequential public-sector AI. The framework should be coordinated with constitutional rights, existing administrative law, data-protection policy and public-procurement rules.

10.9 Strengthen Judicial and Professional AI Literacy

Judges, lawyers, prosecutors and administrators should receive training on model limitations, probabilistic outputs, hallucination risks, data bias, validation and appropriate reliance. Training should support legal judgment rather than encourage technological deference.

10.10 Encourage Interoperable International Standards

International cooperation should focus on baseline governance principles while allowing jurisdictions to adapt rules to constitutional structures, institutional capacity and sector-specific risks.

11. Conclusion

AI is changing legal decision-making, but the legal significance of that change depends on how authority is allocated and constrained. The principal challenge is not simply that algorithms may be inaccurate or opaque. It is that public decisions traditionally justified through identifiable legal rules, reasons and accountable officials can become dependent on complex socio-technical systems involving vendors, datasets, procurement choices and human-machine interaction.

The first research question is therefore answered by distinguishing decision support from decision automation. The second is answered through the analysis of due process, equality, transparency, automation bias, accountability and individualized consideration. The third is answered comparatively: the EU provides a risk-based statutory model; Canada demonstrates structured administrative impact assessment; the Council of Europe provides judicial-sector principles; and U.S. litigation illustrates how existing legal doctrines can constrain algorithmic use without a comprehensive AI statute. None is a complete template for every jurisdiction.

For Pakistan, the constitutional principles of fair trial, equality, dignity, privacy and legality already provide important foundations for scrutinizing consequential automated decisions, while the National AI Policy 2025 establishes a policy direction toward responsible AI. The principal legislative challenge is to convert broad policy commitments into enforceable governance mechanisms where necessary.

The article's central conclusion is consequently institutional rather than technological: consequential public-sector AI should remain embedded in a chain of lawful authority, documented procurement, context-specific validation, meaningful human judgment, reasoned decision-making, continuing audit and effective remedy. AI can assist legal institutions, but it should not become an unreviewable source of public authority.

References

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. *ProPublica*.

Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning: Limitations and opportunities*. fairmlbook.org.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.

Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology, 31*(2), 889–938.

Burrell, J. (2016). How the machine "thinks": Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12.

Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. *Big Data, 5*(2), 153–163. https://doi.org/10.1089/big.2016.0047

Citron, D. K. (2008). Technological due process. *Washington University Law Review, 85*(6), 1249–1313.

Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. *Washington Law Review, 89*(1), 1–33.

Coglianese, C., & Lehr, D. (2017). Regulating by robot: Administrative decision making in the machine-learning era. *Georgetown Law Journal, 105*(5), 1147–1223.

Danziger, S., Levav, J., & Avnaim-Pesso, L. (2011). Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences, 108*(17), 6889–6892.

European Commission for the Efficiency of Justice. (2018). *European ethical charter on the use of artificial intelligence in judicial systems and their environment*. Council of Europe.

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union.

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.

Government of Canada, Treasury Board of Canada Secretariat. (2024). *Directive on automated decision-making*.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: Novel entanglements of law and technology*. Edward Elgar Publishing.

Kleinberg, J., Mullainathan, S., & Raghavan, M. (2016). Inherent trade-offs in the fair determination of risk scores. In *Proceedings of the 8th Innovations in Theoretical Computer Science Conference*.

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705.

Lehr, D., & Ohm, P. (2017). Playing with the data: What legal scholars should learn about machine learning. *UC Davis Law Review, 51*(2), 653–717.

Mayson, S. G. (2019). Bias in, bias out. *Yale Law Journal, 128*(8), 2218–2300.

Ministry of Information Technology and Telecommunication, Government of Pakistan. (2025). *National Artificial Intelligence Policy 2025*.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21.

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). https://doi.org/10.6028/NIST.AI.100-1

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Pakistan. (1973). *Constitution of the Islamic Republic of Pakistan* (as amended).

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence, 1*(5), 206–215.

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. *Fordham Law Review, 87*(3), 1085–1139.

State v. Loomis, 881 N.W.2d 749 (Wis. 2016).

Surden, H. (2014). Machine learning and law. *Washington Law Review, 89*(1), 87–115.

Susskind, R. (2019). *Online courts and the future of justice*. Oxford University Press.

Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. National Institute of Standards and Technology.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99.

Zalnieriute, M., Moses, L. B., & Williams, G. (2019). The rule of law and automation of government decision-making. *Modern Law Review, 82*(3), 425–455.

// DECLARATIONS

▸ **Funding**	This research received no specific grant from any funding agency.
▸ **Conflict of Interest**	The authors declare that they have no known financial or personal conflicts of interest that could have influenced the work reported in this paper.
▸ **Data Availability Statement**	No new data were created or analysed in this study. The article is based on legislation, regulatory and policy instruments, reported judicial decisions and published scholarship cited in the references.
▸ **Ethical Statement**	Ethical approval was not required because the study is a doctrinal and comparative policy analysis of publicly available legal texts, judicial decisions, policy documents and published literature and did not involve human participants.
▸ **AI Use Disclosure**	Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

// JOURNAL POLICIES *JuriSocial Journal of Criminology & Criminal Justice*

01 OPEN ACCESS & LICENCE
All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

02 COPYRIGHT
Authors retain copyright and grant JJCCJ the right of first publication.

03 PEER REVIEW
Every research article undergoes double-blind peer review by at least two independent reviewers.

04 PUBLICATION ETHICS
JJCCJ follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

05 PLAGIARISM POLICY
All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

06 GENERATIVE AI POLICY
AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

07 CORRECTIONS & RETRACTIONS
Errors are corrected through published corrigenda; retractions follow COPE guidelines.

08 ARCHIVING & INDEXING
Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

09 PUBLICATION CHARGES
No article publishing fee charged.

10 DISCLAIMER
The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

SUBMISSIONS & ENQUIRIES [editor@journal-domain.org] ◆ [https://journal-website-url/]