Physical Education, Health and Social Sciences

https://journal-of-social-education.org

E-ISSN: 2958-5996
P-ISSN: 2958-5988

The Role of AI in Criminal Justice: Predictive Policing, Bias, and Due Process

Muhammad Ahsan Iqbal Hashmi [1], Nimra Zafar [2], Dr. Sajid Sultan [3], Esha Fareed [4]

[1] Assistant Professor of Law Bahauddin Zakariya University Multan (Vehari Campus) Email: ahsanhashmi@bzu.edu.pk
[2] Post Graduate School of Legal Studies University of the Punjab, Lahore Email: nimrazafar023@gmail.com
[3] Lecturer in Law Bahauddin Zakariya University Multan (Vehari Campus) Email: sajidsultan@bzu.edu.pk
[4] LLM, Post Graduate School of Legal Studies University of the Punjab, Lahore Email: isha.fareed12@gmail.com
Corresponding Author: Muhammad Ahsan Iqbal Hashmi
Corresponding Author: Nimra Zafar

DOI: https://doi.org/10.63163/jpehss.v3i3.513

Abstract

The use of Artificial Intelligence (AI) in criminal justice systems across the world is transforming past ways of doing things in terms of law enforcement, judicial proceedings, and criminal prevention. More precisely, predictive policing technologies are designed to make policing as efficient as possible by predicting crime patterns and revealing possible perpetrators with the use of machine learning algorithms. Nonetheless, the speed at which such tools are used is causing significant concerns about legality and ethical aspects especially those arising due to bias in algorithms, lack of transparency, and violation of due process of law.

The following paper analyzes the use of AI in contemporary criminal justice systems, its involvement in predictive analytics, its tendency to reproduce systemic favoritism, and the effect in terms of fundamental rights. This paper critically re-assesses global best practices in an interdisciplinary background and with a particular focus upon the changing legal framework in Pakistan through evolving discourse by the academics and the formation of policies. It ends by recommending practical steps to be taken in order to make sure that implementation of AI in the context of criminal justice leads to improvement in the understanding but not diminishment of the idea of fairness, accountability, and legality.

Key Words: Artificial Intelligence (AI), Criminal Justice, Predictive Policing, Algorithmic Bias, Due Process, Facial Recognition, Legal Accountability, Data, Discrimination, Transparency and Explainability, Pakistan Legal Reform

Introduction

Artificial Intelligence (AI) is becoming an inseparable application in different areas, such as health, finance, and education. Nonetheless, it has been most frightening through its use in criminal justice. To be more efficient in surveillance, analysis of evidence, and, most importantly, detecting crimes, law enforcement organizations around the world are implementing AI-based systems. On the one hand, such innovations have the potential to improve decision-making process and use data to make policing more effective; on the other hand, they impose certain serious legal and ethical dilemmas.

The international debate on AI on criminal justice supports the idea with a special focus on the ramifications of due process, equal protection under the law, and the right to be free of arbitrary state actions. Such technologies as predictive policing models and facial recognition systems usually use big data that is potentially based on the historical biases, which quickly leads them to the reinforcement of discriminatory practices. Where laws are weak or erratically applied (as is so common in Pakistan), this leap in technology is likely to increase the existing disparities even before reducing them.[1]

In addition to this, the lack of transparency in most of these AI systems, which is referred to as the black box of systems, contradicts basic legal principles of accountability and transparency. With the number of governments and law enforcement institutions outsourcing particular stages of decision-making to machines growing, rather important questions come to mind: Who is to be blamed in case of a wrongful arrest based on AI-generated faulty predictions? Is there any

[1] Sandra G. Mayson, "Bias In, Bias Out," accessed June 27, 2025, https://www.yalelawjournal.org/article/bias-in-bias-out.

meaningful opportunity of an accused to challenge evidence of algorithms? Is the predictive tool application in line with the constitutional right to a fair trial?[2]

This paper explores these pressing questions by examining the integration of AI into criminal justice systems with a threefold focus: predictive policing, algorithmic bias, and due process. Through this inquiry, it seeks to highlight both the promise and peril of AI, ultimately proposing pathways for legal and policy reform in Pakistan and similar jurisdictions.[3]

The Emergence of AI in Criminal Justice

The incorporation of Artificial Intelligence into criminal justice systems marks a paradigmatic shift in how states conceptualize law enforcement and judicial efficiency. At its core, AI refers to machine-based systems capable of making predictions, recommendations, or decisions by processing vast datasets using complex algorithms. In the context of criminal justice, these capabilities are being utilized to assess risk, monitor populations, allocate police resources, and even influence sentencing decisions.[4]

The emergence of AI in criminal justice is closely tied to advancements in machine learning and big data analytics. These technologies allow systems to identify patterns in historical crime data, which are then used to predict future incidents. For instance, predictive policing tools use crime location and time data to generate "hotspot maps" that suggest where crimes are most likely to occur.[5] Similarly, risk assessment algorithms employed in courts predict the likelihood of recidivism to aid in bail and sentencing decisions.[6] While these applications are designed to improve public safety and judicial efficiency, they have also drawn scrutiny for replicating and amplifying the very biases embedded in historical datasets.

The adoption of AI technologies has been more aggressive in developed jurisdictions like the United States, the United Kingdom, and China. For example, the Los Angeles Police Department's use of the "Operation LASER" program and Chicago's "Strategic Subject List" are among the most cited early experiments in predictive policing.[7] Both programs, however, were eventually suspended due to concerns over racial profiling and civil liberties violations.[8] These international examples offer critical lessons for countries like Pakistan, where the state is increasingly reliant on digital surveillance and centralized data platforms in law enforcement, yet lacks corresponding regulatory oversight.

Practically no adoption of AI-solutions in Pakistan gives the impression that the use of such tools is very limited. This is evidenced by attempts to digitalize records of the police, combine them with the data of the National Database and Registration Authority (NADRA), and use facial recognition at public facilities. There are however, visible lack of laws and institutional frameworks of controlling their use.[9] The nation does not have a single data protection policy, a charter of AI ethics, or a set of court cases with explanations of whether algorithmic decisions are lawful in criminal investigations. This gap in regulation brings dangers of unregulated monitoring, false allegations, and the secrecy of the process that surpass the protection of the constitution.

The role of AI will probably grow in criminal justice as such systems develop further. It is all the more necessary to consider the operating principles of these systems as well as their embedded values and assumptions. The unmoored application of AI in the arena of criminal justice concerned is bound to generate a technological veneer of impartiality as racial, economic, social, and positional disparity are entrenched.

Predictive Policing and Crime Forecasting

The most popular use of AI that is associated with the field of law enforcement is predictive policing. It includes applying statistical algorithms and machine learning models to extract sizeable

---

[2] "Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence," accessed June 27, 2025, https://www.nature.com/articles/s42256-019-0114-4.

[3] Sarah Brayne, "Big Data Surveillance: The Case of Policing," *American Sociological Review* 82, no. 5 (October 2017): 977–1008, https://doi.org/10.1177/0003122417725865.

[4] "Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea | Philosophy & Technology," accessed June 27, 2025, https://link.springer.com/article/10.1007/s13347-020-00403-w.

[5] Brayne, "Big Data Surveillance."

[6] Sandra G. Mayson, "Bias In, Bias Out," accessed June 27, 2025, https://www.yalelawjournal.org/article/bias-in-bias-out.

[7] "(PDF) Reform Predictive Policing," accessed June 27, 2025, https://www.researchgate.net/publication/312900875_Reform_predictive_policing.

[8] Joseph Fishman and Deepa Varadarajan, "Similar Secrets," *University of Pennsylvania Law Review* 167, no. 5 (January 1, 2019): 1051.

[9] Danish, Dr Imran Ali Khan, and Dr Aamir Ullah, "The Role of Artificial Intelligence in Enhancing Social Governance: A Framework for Ethical Implementation and Policy Development in Pakistan," *Journal of Management & Social Science* 1, no. 4 (December 25, 2024): 274–89, https://doi.org/10.63075/9fzpbn74.

amounts of data such as crime reports, arrest logs, and various social media activity to project where crimes will happen or which people are likely to participate in criminal activity in the future.[10] Although it is the most efficient way of preventing crime and assigning resources, the methodology evokes difficult questions of privacy, discrimination, and due process.

Among the most frequently cited systems of predictive policing are the United States-created PredPol for predicting crime-prone areas (so-called crime hotspots) through past data analysis.[11] Theoretically, with these kinds of systems, police can position resources in areas that are likely to occur so that they can prevent that crime. Nevertheless, these technologies have been criticized by many studies in the realms of replicating the preexisting trends of biased policing. Since predictive systems are fed with past crime information, which may encode the biased policing policies disproportionately affecting the racial group, the end product is more likely to perpetuate, instead of alleviating, the disparities in the system.[12]

It has been empirically proven that even such neighborhoods which were historically over-policed, e.g., low-income and minority-populated, are still marked by predictive tools as high-risk areas. That forms a self-fulfilling cycle: the more the community is policed, the more arrests there will be, and the more that will feed back into the system, justifying yet more policing.[13] This reasoning is circular, rendering any striving at objectivity illegitimate, and the consequences of such reasoning can be detrimental to a social life, such as stigmatization and alienation in the communities.

Pakistan is beginning to experiment with forms of predictive policing, particularly in urban centers such as Lahore and Karachi. These efforts include using surveillance footage, facial recognition, and digital profiling to monitor public spaces and predict criminal activity.[14] However, these practices often operate without public awareness, legal authorization, or judicial oversight. Given Pakistan's fragile democratic institutions and limited accountability mechanisms, the risk of abuse is significant.

Moreover, predictive policing can conflict with the constitutional guarantees of equality and fair treatment. Individuals flagged by algorithms may face increased scrutiny or denial of bail without having committed any offense, raising concerns about **pre-crime logic** reminiscent of dystopian narratives.[15] The lack of transparency in how these tools function also limits an individual's ability to challenge the basis of state action, thereby infringing upon procedural safeguards embedded in due process.

Although AI-based crime forecasting may help optimize policing strategies, its current deployment, especially in contexts lacking robust legal oversight, presents substantial risks. As the Pakistani state moves toward digitized law enforcement, it must prioritize the establishment of legal frameworks that balance innovation with constitutional protections.

Algorithmic Bias and Discriminatory Outcomes

While proponents of AI often laud its objectivity and efficiency, the reality is that AI systems, particularly those used in criminal justice, are deeply susceptible to algorithmic bias. These biases are not inherent to the technology itself but are inherited from the data upon which AI systems are trained.[16] In practice, this means that if historical crime data is tainted by racial, socioeconomic, or geographic disparities, AI models built on such data are likely to replicate and reinforce those disparities in their predictions and recommendations.

A major source of algorithmic bias is label bias, where the outcomes used to train the model are themselves the product of biased decision-making. For example, arrest data may overrepresent certain communities not because of higher crime rates but because of disproportionate policing.[17] When AI tools are trained on such data, they infer that people from those communities are more likely to commit crimes, even when no such correlation exists in reality. This leads to unfair risk assessments and discriminatory policing outcomes.

---

[10] "(PDF) Reform Predictive Policing."

[11] Brayne, "Big Data Surveillance."

[12] Sandra G. Mayson, "Bias in, Bias Out," *Yale Law Journal* 128 (2019 2018): 2218.

[13] "To Predict and Serve? | Significance | Oxford Academic," accessed June 27, 2025, https://academic.oup.com/jrssig/article/13/5/14/7029190?login=false.

[14] Gohar Masood Qureshi, Fazail Asrar Ahmed, and Faiza Chaudhary (Corresponding Author), "Algorithmic Justice and Legal Pluralism: Rethinking Artificial Intelligence Regulation in Pakistan's Hybrid Legal System," *Competitive Research Journal Archive* 3, no. 02 (April 26, 2025): 67–75.

[15] "'Gatekeepers Gone Wrong' by Laura N. Coordes," accessed June 27, 2025, https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/6/.

[16] "Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence," accessed June 27, 2025, https://www.nature.com/articles/s42256-019-0114-4.

[17] Solon Barocas and Andrew D. Selbst, "Big Data's Disparate Impact," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 2016), https://doi.org/10.2139/ssrn.2477899.

The U.S.-based COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) algorithm, which is used to assess the likelihood of recidivism, has been one of the most cited examples of algorithmic bias in criminal justice. Studies revealed that COMPAS disproportionately assigned higher risk scores to Black defendants compared to White defendants with similar profiles.[18] The algorithm was proprietary and its internal logic opaque, making it impossible for defendants to challenge its outputs, raising serious concerns about transparency and accountability.[19]

In Pakistan, although the deployment of risk assessment tools like COMPAS has not yet occurred, the increasing use of AI in surveillance and profiling introduces similar risks. Without rigorous audits and bias-mitigation protocols, these systems can unintentionally target religious minorities, ethnic groups, or political activists based on flawed or politicized datasets.[20] Moreover, the absence of comprehensive anti-discrimination laws in Pakistan's technology governance space leaves affected individuals with little legal recourse.

Bias in AI tools also poses significant challenges to procedural fairness, a cornerstone of due process. If an accused individual is detained, denied bail, or subjected to enhanced surveillance based on algorithmic risk assessments, they must be afforded the opportunity to understand and contest the evidence against them.[21] However, most AI systems in use today lack explainability, a condition often referred to as the "black box problem", making it virtually impossible for courts or litigants to evaluate the fairness of the decision-making process.

Thus, algorithmic bias not only undermines the credibility of AI in criminal justice but also threatens the legitimacy of the legal system itself. Ensuring algorithmic fairness requires proactive steps, including the diversification of training datasets, implementation of bias audits, and mandating explainability standards. These reforms must be enshrined in law to prevent the normalization of discriminatory practices under the guise of technological neutrality.

AI and the Right to Due Process

The principle of due process of law is a foundational guarantee in most constitutional democracies, ensuring that individuals are treated fairly and justly by the legal system. As Artificial Intelligence becomes more deeply embedded in criminal justice functions, ranging from predictive policing to risk assessments and facial recognition, the intersection of algorithmic decision-making and due process raises urgent legal concerns.[22]

One of the most pressing issues is the lack of transparency in AI systems used for law enforcement and judicial decision-making. Most advanced AI models function as "black boxes," meaning their internal reasoning is not understandable even to their developers, let alone to legal practitioners or the accused.[23] This opacity directly undermines the right to a fair trial, particularly the accused's right to know and challenge the evidence presented against them. If a judge relies on a risk assessment score generated by a proprietary algorithm to deny bail or impose a harsher sentence, the defendant may have no meaningful way to interrogate the basis of that decision.[24]

This lack of procedural transparency also weakens the principle of equality of arms, whereby both parties in a legal dispute should have equal opportunity to present and contest evidence. In criminal cases where liberty is at stake, the inability to access or understand algorithmic evidence can severely disadvantage defendants, especially in under-resourced legal systems.[25] Furthermore, courts themselves may lack the technical expertise required to scrutinize AI systems or assess the validity of their outputs, leaving room for uncritical acceptance of flawed or biased tools.

---

[18] "Machine Bias — ProPublica," accessed June 27, 2025, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[19] "Machine Bias — ProPublica."

[20] Andrew D Selbst and Julia Powles, "Meaningful Information and the Right to Explanation," *International Data Privacy Law* 7, no. 4 (November 1, 2017): 233–42, https://doi.org/10.1093/idpl/ipx022.

[21] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41 (July 1, 2021): 105567, https://doi.org/10.1016/j.clsr.2021.105567.

[22] Slava (Veaceslav) Balan, "Universal Human Rights Framework and a Global Human Rights Based Approach: What a Regulatory Response to the Rapidly Advancing AI Technologies Should Be?," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, December 12, 2023), https://doi.org/10.2139/ssrn.4662761.

[23] Andrew D Selbst and Julia Powles, "Meaningful Information and the Right to Explanation," *International Data Privacy Law* 7, no. 4 (November 1, 2017): 233–42, https://doi.org/10.1093/idpl/ipx022.

[24] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41 (July 1, 2021): 105567, https://doi.org/10.1016/j.clsr.2021.105567.

[25] Laura Coordes, "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules," *Washington University Law Review* 94, no. 5 (January 1, 2017): 1191–1247.

Another concern is the absence of legal standards governing the admissibility of AI-generated evidence. In Pakistan, the rules of evidence as codified in the Qanun-e-Shahadat Order, 1984, do not specifically address algorithmic evidence or data-driven decision-making.[26] This legal vacuum increases the risk of arbitrary or unlawful use of technology in criminal proceedings. Without clear criteria for validating, authenticating, or challenging algorithmic inputs, such tools may be used without judicial restraint, contravening both domestic and international human rights standards.

In addition, automated decision-making systems can conflict with presumptions of innocence and individualized justice, two key tenets of criminal law. Risk scores that classify individuals as "high-risk" based on their demographic or geographic characteristics can lead to preemptive actions, such as denial of bail or heightened surveillance, based on prediction rather than proof.[27] This predictive logic transforms the criminal justice system from a mechanism of adjudication to one of preemption, eroding the moral and legal foundation of punishment based on culpability.

To uphold due process in the age of AI, legal systems must develop robust regulatory safeguards. These include mandating algorithmic explainability, establishing standards for admissibility, and training judicial actors in the critical evaluation of AI tools. Importantly, defendants must be guaranteed the right to contest algorithmic determinations, including access to the data and models used. Only then can the use of AI in criminal justice align with the constitutional promise of fairness and justice.

Comparative Perspectives: Global Trends and Lessons for Pakistan

The integration of Artificial Intelligence in criminal justice systems is not occurring in a vacuum; rather, it is part of a broader global trend shaped by varying legal, institutional, and political contexts. Comparative analysis reveals both cautionary tales and best practices that can inform Pakistan's approach to regulating AI in criminal law. Countries such as the United States, the United Kingdom, and members of the European Union have faced significant challenges in aligning AI deployment with fundamental rights, but they have also undertaken steps to mitigate harms, offering valuable lessons for emerging jurisdictions.

In the United States, the use of predictive policing tools like PredPol and risk assessment algorithms like COMPAS has been widespread. However, both technologies have come under intense scrutiny for their lack of transparency and discriminatory outcomes.[28] The American legal system's decentralized structure and strong civil society have enabled public interest litigation, investigative journalism, and academic research to hold these systems accountable. For instance, ProPublica's 2016 exposé on COMPAS's racial bias prompted nationwide debates and calls for reform.[29] Yet, despite these efforts, federal-level regulation remains minimal, leaving AI governance largely to state jurisdictions.

The United Kingdom, in contrast, has adopted a more cautious and centralized approach. The London Metropolitan Police's trials with facial recognition technologies were challenged in court, leading to a 2020 ruling by the Court of Appeal that the deployments violated privacy and data protection laws.[30] The UK government and courts have emphasized the need for proportionality, legality, and public oversight when implementing AI technologies in policing. Moreover, the Information Commissioner's Office (ICO) has issued guidance to ensure that automated systems meet data protection standards and allow individuals to contest decisions affecting their rights.[31]

The European Union has gone even further with its proposed AI Act, which seeks to classify AI applications based on their risk levels, prohibiting high-risk uses like social scoring and tightly regulating AI used in law enforcement.[32] The Act also mandates transparency obligations, impact assessments, and accountability mechanisms, aiming to strike a balance between innovation and

---

[26] Gohar Masood Qureshi, Fazail Asrar Ahmed, and Faiza Chaudhary (Corresponding Author), "Algorithmic Justice and Legal Pluralism: Rethinking Artificial Intelligence Regulation in Pakistan's Hybrid Legal System," *Competitive Research Journal Archive* 3, no. 02 (April 26, 2025): 67–75.

[27] "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School," accessed June 27, 2025, https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

[28] "Machine Bias — ProPublica," accessed June 27, 2025, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[29] Laura Coordes, "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules," *Washington University Law Review* 94, no. 5 (January 1, 2017): 1191–1247.

[30] "R. (on the Application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058 (11 August 2020) | Practical Law," accessed June 27, 2025, https://uk.practicallaw.thomsonreuters.com/D-105-0363?transitionType=Default&contextData=(sc.Default)&firstPage=true.

[31] "Guidance on AI and Data Protection" (ICO, January 16, 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

[32] "EUR-Lex - 52021PC0206 - EN - EUR-Lex," accessed June 27, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

fundamental rights. This rights-based, preemptive regulatory approach contrasts with the reactive models of the U.S. and provides a robust blueprint for countries like Pakistan.

In Pakistan, however, AI technologies are being deployed in a largely unregulated and opaque environment. While initiatives such as Safe City Projects and facial recognition systems are expanding, there is little to no public debate, judicial review, or legislative scrutiny of these tools.[33] The absence of a dedicated data protection law, a national AI regulatory authority, and judicial precedent on algorithmic accountability puts Pakistan at a significant disadvantage in addressing the risks associated with AI in criminal justice. Moreover, the existing legal framework—including the Pakistan Electronic Crimes Act (PECA) 2016 and the Qanun-e-Shahadat Order 1984—is ill-equipped to handle the complexities of AI-generated evidence and automated decision-making.

Adopting lessons from the EU and UK, Pakistan must pursue a principle-based legal framework that foregrounds transparency, proportionality, and accountability. This requires legislative reform, judicial activism, and institutional capacity building. Without these steps, AI's potential in Pakistan's criminal justice system may be undermined by unchecked surveillance, systemic bias, and erosion of constitutional safeguards.

Policy Recommendations and Ethical Considerations

As the deployment of Artificial Intelligence in criminal justice accelerates globally and within Pakistan, a coherent legal and ethical framework becomes imperative. Policymakers, judicial authorities, and civil society actors must ensure that innovation in law enforcement does not come at the cost of constitutional rights, especially due process, equality, and accountability.[34] Based on the preceding analysis, this section offers policy recommendations grounded in legal ethics and comparative best practices.

Enact Comprehensive Data Protection Legislation

The absence of a unified data protection law in Pakistan leaves individuals vulnerable to misuse of personal data by state and private actors. Without such legislation, there are no safeguards over the collection, storage, or processing of biometric and behavioral data used by AI systems in surveillance or profiling.[35] The proposed Personal Data Protection Bill, still pending as of 2025, should be expedited and expanded to explicitly cover AI and automated decision-making systems. The law must also ensure data minimization, purpose limitation, and enforceable rights to access and rectify data.

Mandate Algorithmic Transparency and Explainability

Transparency in AI systems is essential for preserving due process.[36] Legal actors—particularly judges and defense counsel—must be able to understand and interrogate the logic behind AI-generated risk scores or policing recommendations. To that end, Pakistan should adopt algorithmic explainability requirements, similar to those proposed in the European Union's AI Act.[37] These rules should require vendors and state agencies to disclose the functioning, datasets, and limitations of AI systems used in criminal justice.

Establish an AI Oversight Authority

Given the rapid pace of technological integration, a dedicated AI regulatory authority should be established. This body should include legal experts, technologists, ethicists, and civil society members. Its mandate should cover licensing, compliance audits, impact assessments, and the investigation of public complaints related to AI misuse.[38] Institutionalizing such oversight would prevent unchecked implementation and ensure that AI tools meet constitutional and ethical standards before deployment.

---

[33] "EUR-Lex - 52021PC0206 - EN - EUR-Lex."

[34] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41 (July 1, 2021): 105567, https://doi.org/10.1016/j.clsr.2021.105567.

[35] Wachter, Mittelstadt, and Russell.

[36] "Meaningful Information and the Right to Explanation | International Data Privacy Law | Oxford Academic," accessed June 27, 2025, https://academic.oup.com/idpl/article-abstract/7/4/233/4762325?redirectedFrom=fulltext.

[37] "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS" (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[38] "Guidance on AI and Data Protection" (ICO, January 16, 2025), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

Introduce Judicial Guidelines for AI Use in Criminal Cases

Judicial discretion in Pakistan must be supplemented with clear procedural guidance on the admissibility, probative value, and limits of AI-generated evidence. The Supreme Court of Pakistan could issue practice directions—similar to the UK's Criminal Practice Rules—to guide lower courts.[39] These guidelines should emphasize that AI-generated outputs are not infallible and must be corroborated by traditional evidence.

Build Institutional Capacity and Legal Literacy

The effective regulation of AI in criminal justice also depends on the capacity of legal institutions. Judges, prosecutors, and defense attorneys must be trained in the basics of AI systems, including their strengths, weaknesses, and legal implications. Legal education curricula should incorporate technology law and ethics, and bar associations should provide continuing education programs on emerging AI-related issues.[40]

Promote Ethical AI Design and Procurement Standards

Government agencies procuring AI tools must adopt ethical design principles, including fairness, non-discrimination, and human oversight. Public procurement contracts should mandate third-party audits for bias and transparency. Moreover, no AI system should be used in criminal justice without a human-in-the-loop mechanism, ensuring that decisions affecting fundamental rights are not automated entirely.[41]

Ethically guided AI in criminal justice is not merely a technological imperative; it is a constitutional and moral necessity. If Pakistan aims to reap the benefits of AI without deepening its systemic inequalities, it must embed rights-based considerations into the very architecture of these systems.

Conclusion

Artificial intelligence in the criminal justice is the sword with two edges: on the one hand, it promises to provide more efficiency, consistency, and evidence-based decision making but on the other hand, it poses serious threats of eroding essential legal rights. Left unchecked, predictive policing tools, risk assessment algorithms and AI-powered surveillance systems can be tools used to solidify built-in biases, conceal responsibility and undermine the critical principles of due process.

In this paper, the essential aspects of the integration of AI in criminal justice were discussed, namely the predictive policing, algorithmic bias, and due process. Experience in different jurisdictions like the United States, the United Kingdom and the European Union suggests that technological innovations are an unavoidable development, but then it should be governed by good legal provisions and ought to be subjected to institutional controls and judicial oversight. In the case of Pakistan, the lessons are more pressing: the early implementation of AI without corresponding protection mechanisms might further exclude the vulnerable groups and undermine the justice system.

To protect constitutional interests' numerous measures, have to be taken in Pakistan to have well-rounded data protection laws, clear AI governmental systems, and court rules that support fairness, and accountability. Ethical AI is more than a technically desirable construct; it is a law requiring construct. Since the state continues its process of digitalizing law enforcement and judicial processes, its interest is to make sure that innovation will not be a new domain to implement injustice, but to renew the rule of law.

References

Balan, Slava (Veaceslav). "Universal Human Rights Framework and a Global Human Rights Based Approach: What a Regulatory Response to the Rapidly Advancing AI Technologies Should Be?" SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, December 12, 2023. https://doi.org/10.2139/ssrn.4662761.

Barocas, Solon, and Andrew D. Selbst. "Big Data's Disparate Impact." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 2016. https://doi.org/10.2139/ssrn.2477899.

[39] Laura Coordes, "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules," *Washington University Law Review* 94, no. 5 (January 1, 2017): 1191–1247.

[40] "Big Data's Disparate Impact by Solon Barocas, Andrew D. Selbst :: SSRN," accessed June 27, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

[41] "Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence," accessed June 27, 2025, https://www.nature.com/articles/s42256-019-0114-4.

"Beyond a Human Rights-Based Approach to AI Governance: Promise, Pitfalls, Plea | Philosophy & Technology." Accessed June 27, 2025. https://link.springer.com/article/10.1007/s13347-020-00403-w.

"Big Data's Disparate Impact by Solon Barocas, Andrew D. Selbst :: SSRN." Accessed June 27, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.

Brayne, Sarah. "Big Data Surveillance: The Case of Policing." American Sociological Review 82, no. 5 (October 2017): 977–1008. https://doi.org/10.1177/0003122417725865.

Coordes, Laura. "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules." Washington University Law Review 94, no. 5 (January 1, 2017): 1191–1247.

———. "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules." Washington University Law Review 94, no. 5 (January 1, 2017): 1191–1247.

———. "Gatekeepers Gone Wrong: Reforming the Chapter 9 Eligibility Rules." Washington University Law Review 94, no. 5 (January 1, 2017): 1191–1247.

Danish, Dr Imran Ali Khan, and Dr Aamir Ullah. "The Role of Artificial Intelligence in Enhancing Social Governance: A Framework for Ethical Implementation and Policy Development in Pakistan." Journal of Management & Social Science 1, no. 4 (December 25, 2024): 274–89. https://doi.org/10.63075/9fzpbn74.

"EUR-Lex - 52021PC0206 - EN - EUR-Lex." Accessed June 27, 2025. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

Fishman, Joseph, and Deepa Varadarajan. "Similar Secrets." University of Pennsylvania Law Review 167, no. 5 (January 1, 2019): 1051.

"'Gatekeepers Gone Wrong' by Laura N. Coordes." Accessed June 27, 2025. https://openscholarship.wustl.edu/law_lawreview/vol94/iss5/6/.

"Guidance on AI and Data Protection." ICO, January 16, 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

"Guidance on AI and Data Protection." ICO, January 16, 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/.

"Machine Bias — ProPublica." Accessed June 27, 2025. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

"Machine Bias — ProPublica." Accessed June 27, 2025. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

Mayson, Sandra G. "Bias in, Bias Out." Yale Law Journal 128 (2019 2018): 2218.

———. "Bias In, Bias Out." Accessed June 27, 2025. https://www.yalelawjournal.org/article/bias-in-bias-out.

———. "Bias In, Bias Out." Accessed June 27, 2025. https://www.yalelawjournal.org/article/bias-in-bias-out.

"Meaningful Information and the Right to Explanation | International Data Privacy Law | Oxford Academic." Accessed June 27, 2025. https://academic.oup.com/idpl/article-abstract/7/4/233/4762325?redirectedFrom=fulltext.

"(PDF) Reform Predictive Policing." Accessed June 27, 2025. https://www.researchgate.net/publication/312900875_Reform_predictive_policing.

"Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence." Accessed June 27, 2025. https://www.nature.com/articles/s42256-019-0114-4.

"Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence." Accessed June 27, 2025. https://www.nature.com/articles/s42256-019-0114-4.

"Principles Alone Cannot Guarantee Ethical AI | Nature Machine Intelligence." Accessed June 27, 2025. https://www.nature.com/articles/s42256-019-0114-4.

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (2021). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

Qureshi, Gohar Masood, Fazail Asrar Ahmed, and Faiza Chaudhary (Corresponding Author). "Algorithmic Justice and Legal Pluralism: Rethinking Artificial Intelligence Regulation in Pakistan's Hybrid Legal System." Competitive Research Journal Archive 3, no. 02 (April 26, 2025): 67–75.

———. “Algorithmic Justice and Legal Pluralism: Rethinking Artificial Intelligence Regulation in Pakistan’s Hybrid Legal System.” Competitive Research Journal Archive 3, no. 02 (April 26, 2025): 67–75.

“R. (on the Application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058 (11 August 2020) | Practical Law.” Accessed June 27, 2025. https://uk.practicallaw.thomsonreuters.com/D-105-0363?transitionType=Default&contextData=(sc.Default)&firstPage=true.

Selbst, Andrew D, and Julia Powles. “Meaningful Information and the Right to Explanation.” International Data Privacy Law 7, no. 4 (November 1, 2017): 233–42. https://doi.org/10.1093/idpl/ipx022.

———. “Meaningful Information and the Right to Explanation.” International Data Privacy Law 7, no. 4 (November 1, 2017): 233–42. https://doi.org/10.1093/idpl/ipx022.

“The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Book - Faculty & Research - Harvard Business School.” Accessed June 27, 2025. https://www.hbs.edu/faculty/Pages/item.aspx?num=56791.

“To Predict and Serve? | Significance | Oxford Academic.” Accessed June 27, 2025. https://academic.oup.com/jrssig/article/13/5/14/7029190?login=false.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. “Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI.” Computer Law & Security Review 41 (July 1, 2021): 105567. https://doi.org/10.1016/j.clsr.2021.105567.

———. “Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI.” Computer Law & Security Review 41 (July 1, 2021): 105567. https://doi.org/10.1016/j.clsr.2021.105567.

———. “Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI.” Computer Law & Security Review 41 (July 1, 2021): 105567. https://doi.org/10.1016/j.clsr.2021.105567.