Safeguarding Human Rights in the Age of Artificial Intelligence: Evaluating the Adequacy of Legal Frameworks in criminal justice

Zainab Buba
Department of General Studies
Katsina State Institute of Technology and Management (KSITM)
Email; zeebuba2020@gmail.com

Phone no; 07031014580

DOI : https://doi.org/10.5281/zenodo.17387365

ABSTRACT
The integration of Artificial Intelligence (AI) into criminal justice systems is reshaping law enforcement, adjudication, and corrections. From predictive policing to algorithmic risk assessments and sentencing recommendations, AI tools promise increased efficiency and consistency. However, their deployment raises critical legal and ethical concerns. This paper examines the impact of AI through the lens of fairness, accountability, transparency, and human rights, focusing on issues such as algorithmic bias, model opacity, and the reinforcement of systemic inequalities. It assesses whether existing legal frameworks constitutional protections, data privacy laws, and international human rights standards offer adequate safeguards. Drawing on comparative insights from jurisdictions using AI in justice, the analysis underscores both opportunities and risks, and calls for robust regulation and ethical oversight. The paper concludes that without strong legal safeguards, AI risks undermining fundamental rights and public trust in the justice system.

Keywords: *Artificial Intelligence (AI), Criminal Justice, Algorithmic Bias, Human Rights, Legal Safeguards*

1. Introduction

Artificial Intelligence (AI) has emerged as one of the defining technologies of the twenty-first century, reshaping economies, governance, and social life. Its integration into criminal justice systems represents both an unprecedented opportunity and a substantial challenge. Law enforcement agencies, courts, and correctional institutions are increasingly adopting AI-driven tools such as predictive policing software, risk assessment algorithms, facial recognition technologies, and automated sentencing systems (Bryson, 2020). Advocates argue that such innovations enhance efficiency, reduce costs, and provide greater consistency in decision-making. However, critics caution that AI adoption in criminal justice risks entrenching existing inequalities, undermining human rights, and eroding public trust in the rule of law (Ferguson, 2017; Angwin et al., 2016; Barocas & Selbst, 2016).

The core dilemma lies in the tension between technological innovation and the protection of fundamental rights. AI systems, while often promoted as objective, are not immune to bias; numerous studies show that predictive policing and risk assessment tools disproportionately target marginalized communities, reproducing systemic discrimination embedded in historical data. These concerns are amplified in contexts where institutional safeguards are weak or unevenly enforced, raising urgent questions about fairness, transparency, and accountability.

Recent legal and policy developments underscore the global dimensions of this debate. In the Global North, the European Union's Artificial Intelligence Act (2024) has introduced the world's first comprehensive regulatory framework, prohibiting high-risk practices such as predictive policing and mandating robust oversight of justice-related AI systems. In the Global South, Nigeria's Data Protection Act (2023) establishes a national legal foundation for safeguarding digital rights, including limits on automated decision-making, while exposing persistent challenges of enforcement capacity and digital exclusion. African scholarship and policy dialogues, such as UNESCO's 2025 East Africa forum on AI and the rule of law, further highlight the need for locally grounded approaches that avoid Eurocentric framings of justice and rights.

This study situates the use of AI in criminal justice within these intersecting debates, drawing on both Global North and Global South perspectives. By examining how emerging legal frameworks, socio-technical realities, and human rights concerns converge, it aims to illuminate the promises and perils of deploying AI in justice systems, and to assess the extent to which regulatory models can balance innovation with equity and accountability.

From a legal perspective, the deployment of AI in criminal justice intersects with constitutional guarantees, statutory protections, and international human rights frameworks. Central to this debate are questions of fairness, accountability, and transparency. Do existing legal frameworks sufficiently safeguard against algorithmic harms? If not, what reforms are necessary to ensure that AI serves the cause of justice rather than undermines it? Addressing these questions requires a careful examination of current laws, an analysis of case studies from different jurisdictions, and a forward-looking discussion of regulatory and ethical approaches.

The significance of this inquiry cannot be overstated. Criminal justice systems wield immense power over individual lives, liberty, and dignity. Any technology integrated into such systems must therefore meet the highest standards of fairness and accountability. Unlike commercial applications of AI, where errors may result in financial loss or reputational harm, errors in criminal justice contexts may result in wrongful arrests, unjust convictions, or disproportionate

sentencing. As such, the stakes of AI governance in this domain are uniquely high (Crawford, 2021).

This paper proceeds in seven parts. Following this introduction, Part Two provides an overview of AI applications in criminal justice, highlighting both domestic and international examples. Part Three examines the potential opportunities of AI, particularly its contributions to efficiency, consistency, and crime prevention. Part Four explores the legal and ethical concerns surrounding AI use, with attention to bias, transparency, accountability, and due process. Part Five evaluates the adequacy of existing legal frameworks, analysing constitutional protections, data protection regimes, and international human rights obligations. Part Six proposes pathways toward stronger legal safeguards, emphasizing principles of fairness, accountability, and transparency, alongside regulatory and policy reforms. Finally, Part Seven concludes with reflections on balancing technological innovation with the imperatives of justice and human rights.

By situating AI within the broader discourse of law, technology, and society, this paper contributes to an urgent and evolving debate. It seeks to illuminate not only the risks of unchecked AI adoption but also the opportunities for harnessing technology in service of a more equitable and effective criminal justice system.

2. Artificial Intelligence in Criminal Justice: An Overview

Artificial Intelligence is increasingly woven into the fabric of modern criminal justice systems, where it is deployed across the spectrum of law enforcement, adjudication, and corrections. AI in this context generally refers to computer systems capable of analysing vast amounts of data, identifying patterns, and making predictions or recommendations that inform decision-making. While such systems promise efficiency and enhanced accuracy, their application in criminal justice is uniquely sensitive due to the high stakes involved—personal liberty, human dignity, and societal trust in legal institutions.

2.1 Predictive Policing

Predictive policing is among the most prominent applications of AI in criminal justice. It involves using historical crime data and machine-learning algorithms to forecast where crimes are likely to occur or who might be at risk of committing or experiencing crime (Perry, McInnis, Price, Smith, & Hollywood, 2013). Police departments in cities such as Los Angeles, Chicago, and London have experimented with predictive policing tools like PredPol and HunchLab.

While these programs claim to optimize resource allocation and reduce crime rates, empirical studies reveal mixed outcomes. In practice, predictive policing often reflects and amplifies existing biases in policing data, disproportionately targeting minority communities already subject to over-policing (Lum & Isaac, 2016). This dynamic not only perpetuates cycles of criminalization but also raises concerns about equal protection under the law and the right to non-discrimination.

2.2 Risk Assessment Tools

Another key application of AI is in risk assessment instruments used during pretrial, sentencing, and parole decisions. Tools such as the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) in the United States are designed to predict the likelihood of reoffending. Judges and parole boards rely on these assessments to inform decisions about bail, sentencing length, and parole eligibility.

Although risk assessments are promoted as objective alternatives to human judgment, research indicates that they are susceptible to significant error and bias. A landmark investigation by ProPublica found that COMPAS disproportionately overestimated recidivism risk for Black defendants while underestimating it for White defendants (Angwin et al., 2016). Such outcomes undermine the fairness of sentencing and challenge the foundational legal principle of equality before the law.

2.3 Facial Recognition Technologies

Facial recognition software represents another controversial application of AI in criminal justice. Law enforcement agencies use these systems for surveillance, suspect identification, and forensic investigations. Countries such as China have adopted facial recognition extensively for public security purposes, while police forces in the United States and Europe have deployed it in varying degrees.

However, numerous studies highlight the inaccuracy of facial recognition, particularly in identifying women, people of colour, and younger individuals (Buolamwini & Gebru, 2018). Misidentification can lead to wrongful arrests and prosecutions, posing significant risks to due process and personal liberty. Furthermore, widespread surveillance facilitated by facial recognition technology raises pressing questions about privacy rights and proportionality in democratic societies.

2.4 Automated Sentencing and Decision Support

Some jurisdictions are exploring AI systems to provide decision-support tools for judges. These tools may recommend sentencing ranges, assess flight risk, or suggest alternatives to incarceration. Proponents argue that automation can reduce disparities caused by human bias, while critics contend that embedding algorithms into sentencing may entrench rather than mitigate inequalities (Binns, 2019).

Moreover, reliance on automated recommendations challenges judicial independence and discretion. If judges defer excessively to algorithmic outputs, accountability for sentencing decisions may become obscured. This undermines the principle that justice must not only be done but must also be seen to be done.

2.5 Comparative perspectives

The deployment of AI in criminal justice varies significantly across jurisdictions. In the United States, adoption is largely decentralized, with local police departments and state courts experimenting with different tools. In contrast, the European Union has adopted a more cautious approach, emphasizing fundamental rights and proposing stringent regulations under the draft Artificial Intelligence Act (European Commission, 2021). China, by comparison, has

embraced AI widely in law enforcement and judicial processes, reflecting its broader model of governance and surveillance.

These divergent approaches illustrate the global patchwork of AI governance. While some jurisdictions prioritize innovation and efficiency, others stress human rights protections. The comparative analysis underscores the urgent need for international dialogue and cooperation to develop common principles that reconcile technological advancement with the imperatives of justice. In sum, AI is already embedded in various facets of criminal justice, from predictive policing to facial recognition and risk assessment. Each application carries potential benefits but also significant risks, particularly in relation to fairness, accountability, and human rights. Understanding these technologies and their real-world consequences is essential for evaluating their compatibility with the rule of law and for developing appropriate regulatory response. Opportunities of AI in Criminal Justice

The adoption of Artificial Intelligence (AI) in criminal justice is not without justification. Proponents emphasize that AI-driven tools have the potential to enhance efficiency, improve consistency, and enable data-driven strategies that can transform how justice systems operate. These opportunities, if harnessed responsibly, could contribute to fairer and more effective outcomes in law enforcement, adjudication, and corrections.

3.1 Efficiency and Resource Optimization

Criminal justice systems worldwide often struggle with resource constraints, ranging from understaffed police departments to overburdened courts. AI tools offer a means of optimizing limited resources by automating routine tasks and enabling faster decision-making. Predictive policing, for instance, allows law enforcement agencies to allocate personnel more strategically, concentrating efforts in areas where crimes are statistically more likely to occur (Perry et al., 2013). Similarly, automated document review systems can assist prosecutors and defence attorneys by rapidly analysing large volumes of evidence, reducing delays in trials.

In correctional facilities, AI-driven monitoring systems can enhance security while reducing labour costs. These efficiencies do not merely represent cost savings; they may also translate into shorter case backlogs, faster adjudication, and improved access to justice for individuals awaiting trial.

3.2 Enhancing Consistency and Objectivity

One of the most compelling arguments in favor of AI adoption is its potential to reduce human bias and inconsistency. Human decision-makers in criminal justice—police officers, judges, parole boards—are susceptible to subjective biases, fatigue, and error. AI systems, by contrast, apply standardized algorithms to similar cases, theoretically ensuring greater consistency across decisions (Bryson, 2020). For example, sentencing algorithms may help establish uniformity by recommending penalties based on structured criteria rather than personal discretion. In jurisdictions where disparities in sentencing for similar crimes have eroded public trust, algorithmic tools could play a corrective role by curbing arbitrary variations.

However, in Nigeria, the introduction of AI into criminal justice raises distinctive risks that differ from the Western contexts in which most studies have been conducted. Predictive policing, for instance, could entrench existing policing patterns that already disproportionately target certain ethnic or regional groups. Nigeria's history of security operations in the Niger

Delta, the North-East, and conflict-prone Middle Belt illustrates how policing is often interwoven with ethnic and political tensions (Akinola, 2020; HRW, 2020). If predictive algorithms are trained on historical arrest and crime data, they are likely to replicate and amplify these biases, reinforcing ethnic profiling and deepening mistrust between communities and law enforcement.

Moreover, Nigeria's criminal justice institutions face persistent challenges of weak oversight, limited transparency, and inconsistent enforcement of rights protections. Judicial review mechanisms are often slow, under-resourced, or inaccessible to marginalized defendants (Okagbue, 2021). In such a context, the opacity of AI "black box" systems could further erode accountability, as defendants may lack effective avenues to contest algorithmic decisions. This risk is compounded by gaps in the enforcement capacity of the Nigeria Data Protection Commission, which is still developing the expertise and infrastructure necessary to audit AI-driven systems under the Data Protection Act (Federal Republic of Nigeria, 2023; ThisDayLive, 2025).

Thus, while algorithmic tools hold promise for promoting consistency, their deployment in Nigeria could reinforce rather than correct systemic inequities if not carefully regulated. Far from eliminating bias, predictive policing and risk assessment systems may harden pre-existing divisions, exacerbating inter-ethnic tensions and weakening already fragile trust in the rule of law.

3.3 Data-Driven Crime Prevention

The predictive capacity of AI is particularly valuable for crime prevention. By analysing large datasets—including crime statistics, socioeconomic indicators, and spatial patterns—AI can identify trends that inform proactive interventions. Predictive policing, when carefully regulated, may allow authorities to address emerging crime "hotspots" before incidents occur, thereby improving public safety (Lum & Isaac, 2016). Additionally, AI can enhance investigative capabilities by identifying links in complex data sets, such as connections between financial transactions in money-laundering cases or communications in organized crime networks. This ability to uncover hidden patterns may empower law enforcement to dismantle criminal enterprises more effectively.

Yet, the risks of predictive policing in Nigeria diverge significantly from those documented in Western contexts. Historical patterns of policing in Nigeria reveal systemic ethnic profiling and regional disparities in law enforcement. Security operations in the Niger Delta, counterterrorism campaigns in the North-East, and farmer–herder conflicts in the Middle Belt have long been shaped by ethnic and political fault lines (Akinola, 2020; HRW, 2020). If predictive algorithms are trained on such datasets, they could disproportionately flag Hausa-Fulani communities in the North, Ijaw and Ogoni groups in the Delta, or Tiv farmers in the Middle Belt as "high risk." In a society where policing already suffers from accusations of bias and selective enforcement, algorithmic policing may harden ethnic stereotypes, deepen intercommunal grievances, and risk inflaming tensions in already volatile regions.

These dangers are magnified by Nigeria's policing practices and weak judicial oversight. The Nigeria Police Force has triggered the nationwide #EndSARS protests (Amnesty International, 2020). Embedding such practices into algorithmic systems risks automating discrimination at scale, lending a veneer of "scientific objectivity" to biased outcomes. Furthermore, Nigeria's judiciary lacks the capacity to provide timely oversight. Chronic delays, underfunding, and

restricted access to legal remedies mean that defendants may find it nearly impossible to challenge algorithmically generated "risk scores" or predictive policing decisions (Okagbue, 2021). The opacity of AI "black box" systems further compounds this problem, as neither defendants nor courts are likely to access the logic driving such outputs.

3.4 Supporting Judicial Decision-Making

AI can serve as a decision-support tool for judges and legal practitioners. Risk assessment systems, for example, provide data-driven evaluations of a defendant's likelihood of reoffending, which may assist in bail and parole determinations. While such systems are not free from controversy, they can supplement judicial reasoning by offering perspectives grounded in statistical analysis (Barocas & Selbst, 2016). In the United States, however, the COMPAS tool has been criticized for racially biased outcomes, raising constitutional concerns about due process in *State v. Loomis* (2016). These global experiences highlight the risks of uncritical adoption and provide important lessons for Nigeria.

In Nigeria, the judicial context presents distinctive challenges. Chronic case backlogs, underfunding, and shortages of trained personnel often pressure judges to seek efficiency at the expense of deliberation (Okagbue, 2021). Against this backdrop, there is a real danger that algorithmic outputs may be treated as authoritative, reducing judges to "rubber stamps" for opaque technologies. This could erode the constitutional right to fair hearing under Section 36 of the 1999 Constitution, especially where defendants lack the resources to contest adverse scores.

Nigeria's justice system is also shaped by longstanding ethnic, socio-economic, and regional disparities. Patterns of harsher pre-trial detention for young men from marginalized communities, as documented during the #EndSARS protests, risk being amplified if encoded into algorithmic models (Amnesty International, 2020; Akinola, 2020). An algorithm trained on such data may systematically classify certain groups—such as urban youth in Lagos or minority populations in conflict-prone areas—as "high risk," reinforcing discriminatory practices under the guise of objectivity.

Beyond risk assessments, natural language processing (NLP) tools could improve judicial efficiency by helping judges, lawyers, and self-represented litigants navigate statutes and precedents. In principle, this could reduce information asymmetries in a system where many defendants lack adequate legal representation. However, Nigeria's uneven digital infrastructure, limited ICT capacity in many courts, and persistent digital exclusion of rural populations raise the risk that AI-enabled legal research may widen, rather than bridge, gaps in access to justice (UNESCO, 2025).

These challenges suggest that AI in judicial decision-making is not simply a technical question but a governance issue. Without safeguards, the technology could undermine, rather than strengthen, Nigeria's justice system. Effective adoption requires:

1. **Mandatory transparency standards**, including disclosure of algorithmic logic in judicial contexts.
2. **Bias and impact assessments** before deploying AI in bail, parole, or sentencing decisions.
3. **Judicial training** to ensure judges understand AI outputs as advisory, not determinative.

4. **Investment in digital infrastructure** to avoid deepening inequalities in access to justice.

Thus, while AI-enabled decision-support tools hold promise, Nigeria's institutional weaknesses mean that their unregulated use could entrench systemic bias and undermine constitutional guarantees. Careful design, strong oversight, and alignment with human rights norms are essential if AI is to serve as a tool for justice rather than a new layer of inequality.

3.5 Advancing Transparency and Accountability (Potentially)

Although often criticized for their opacity, AI systems also hold the potential to advance transparency in some contexts. When designed with explain ability features, algorithms can document the reasoning process behind decisions more consistently than humans, whose motivations may be opaque or unrecorded. This capacity for systematic documentation could facilitate review and oversight, provided that algorithms are subject to rigorous auditing (Binns, 2019).

For example, automated sentencing tools that log their decision-making criteria could create auditable trails, making it easier to detect inconsistencies or biases compared to purely human judgments. Thus, under the right conditions, AI may strengthen rather than weaken accountability.

3.6 Comparative Benefits across Jurisdictions

Different legal systems stand to benefit from AI in distinct ways. In developed jurisdictions, AI may primarily enhance efficiency and uniformity in systems already flush with resources. In developing contexts, where criminal justice institutions may suffer from chronic underfunding and case backlogs, AI could provide transformative gains in access to justice by reducing workload burdens and supporting overstretched personnel (Crawford, 2021).

Furthermore, cross-border applications of AI, such as international cooperation in combating cybercrime or terrorism, illustrate its potential to augment global security efforts. By facilitating collaboration across jurisdictions, AI can contribute to more coordinated responses to transnational threats.

3.7 Summary

The opportunities presented by AI in criminal justice are significant. From optimizing resource allocation and promoting consistency to enhancing predictive capabilities and supporting judicial decisions, AI technologies offer the promise of a more efficient and equitable system. However, these benefits are not automatic. They are contingent upon careful design, rigorous oversight, and alignment with legal and ethical standards. Without such safeguards, the very advantages AI purports to deliver may be undermined by unintended harms.

4. Legal and Ethical Concerns

While Artificial Intelligence (AI) offers compelling opportunities for improving efficiency and consistency in criminal justice systems, it also raises profound legal and ethical challenges. Because criminal justice involves decisions that directly affect individual liberty and fundamental rights, the risks associated with AI adoption are particularly acute. These concerns

can be grouped into five broad categories: algorithmic bias, transparency and explain ability, accountability and liability, due process and fair trial rights, and privacy and surveillance.

4.1 Algorithmic Bias and Discrimination

One of the most pervasive criticisms of AI in criminal justice is its susceptibility to bias. AI systems learn from historical data, which often reflects entrenched patterns of discrimination in policing, sentencing, and corrections. As a result, algorithms may reproduce and even exacerbate systemic inequalities.

The most cited example is the COMPAS risk assessment tool in the United States. A 2016 ProPublica investigation revealed that COMPAS systematically overestimated the likelihood of recidivism for Black defendants while underestimating risk for White defendants (Angwin et al., 2016). This disparity not only undermines fairness but also contravenes the principle of equal protection under the law.

Bias has also been documented in predictive policing systems. By relying on historical crime data that disproportionately reflects arrests in minority communities, predictive policing directs law enforcement resources back to those same areas, creating a feedback loop of over-policing (Lum & Isaac, 2016). Such practices risk reinforcing racial and socioeconomic inequalities, raising concerns under constitutional and human rights law.

Transparency is central to the legitimacy of legal systems, yet many AI tools function as "black boxes." Their underlying algorithms are often proprietary, complex, and inaccessible, even to experts. This opacity poses a serious challenge in legal contexts where decisions must be reviewable and subject to challenge.

For instance, when risk assessment tools influence bail or sentencing, defendants and their counsel may lack the ability to scrutinize how risk scores were calculated. Without access to the underlying logic, contesting these outcomes becomes nearly impossible, undermining due process rights (Goodman & Flaxman, 2017).

The issue is further complicated by trade secrecy claims. Technology companies often refuse to disclose algorithmic details on the grounds of protecting intellectual property. Courts have been divided on whether such claims outweigh defendants' rights to a fair trial. In *State v. Loomis* (2016), the Wisconsin Supreme Court allowed the use of COMPAS in sentencing, despite acknowledging its opacity, provided it was not the sole basis for the decision. This compromise illustrates the legal system's struggle to balance innovation with transparency.

4.3 Accountability and Liability

Accountability is a cornerstone of justice, yet AI challenges traditional frameworks of legal responsibility. When an algorithm produces a flawed recommendation—such as a miscalculated risk score leading to unjust sentencing—who should be held accountable? The judge who relied on the tool, the developer who designed it, or the institution that adopted it?

Current legal systems are ill-equipped to address such questions. In many jurisdictions, accountability is diffused across multiple actors, creating a vacuum of responsibility. This lack of clarity risks eroding public trust, as victims of algorithmic errors may struggle to identify a responsible party.

The European Union's draft Artificial Intelligence Act (2021) attempts to address this gap by classifying AI used in criminal justice as "high-risk" and imposing strict obligations on developers and deployers. These include requirements for human oversight, transparency, and risk management. While promising, the success of such frameworks will depend on effective enforcement mechanisms and international coordination.

4.4 Due Process and Fair Trial Rights

AI adoption in criminal justice also implicates fundamental rights to due process and a fair trial. These rights, enshrined in instruments such as Article 14 of the International Covenant on Civil and Political Rights (ICCPR) and Article 6 of the European Convention on Human Rights (ECHR), require that individuals understand and be able to challenge decisions affecting their liberty.

When algorithms influence bail, sentencing, or parole decisions, defendants may face restrictions without meaningful recourse to contest the basis of those decisions. For example, a defendant denied bail based on an opaque risk score may lack access to the algorithmic reasoning, depriving them of the opportunity to challenge the evidence against them. Such practices are inconsistent with the principle of "equality of arms" in adversarial proceedings (Mayson, 2019).

Automated facial recognition introduces additional risks to due process. In the United Kingdom, civil liberties groups have challenged the police use of live facial recognition, arguing that misidentifications can result in unlawful arrests. The Court of Appeal in *Bridges v. South Wales Police* (2020) ruled that the deployment of facial recognition technology violated privacy rights and data protection laws, underscoring the tension between innovation and human rights in liberal democracies.

4.5 Privacy and Surveillance Concerns

AI technologies, particularly facial recognition and predictive analytics, raise profound concerns about privacy and mass surveillance. Law enforcement agencies equipped with AI-driven surveillance tools can monitor individuals on a scale previously unimaginable. While such capabilities may enhance security, they also threaten the right to privacy guaranteed under international human rights law (Article 17 ICCPR; Article 8 ECHR).

China's widespread use of AI surveillance exemplifies these risks. Integrated systems of facial recognition, biometric data, and predictive analytics have been deployed for social control, sparking criticism from human rights organizations. Although democratic societies typically adopt more restrained approaches, the increasing use of AI surveillance in public spaces blurs the line between legitimate security measures and disproportionate intrusions on individual freedoms (Crawford, 2021).

Data protection regimes such as the EU's General Data Protection Regulation (GDPR) offer some safeguards, including principles of necessity, proportionality, and purpose limitation. However, many jurisdictions lack robust privacy protections, leaving citizens vulnerable to intrusive surveillance practices.

4.6 Broader Ethical Implications

Beyond specific legal issues, the use of AI in criminal justice raises broader ethical questions about the role of technology in society. Should decisions about liberty and punishment ever be delegated to machines, even partially? Does reliance on algorithms risk dehumanizing justice by prioritizing efficiency over compassion and context? Critics argue that justice is not merely a matter of accurate prediction but also of moral judgment, which AI systems are ill-equipped to provide (Bryson, 2020).

These concerns are not merely theoretical. Public trust in criminal justice institutions depends on their perceived fairness and legitimacy. If individuals believe that justice is administered by opaque algorithms rather than accountable human actors, confidence in the rule of law may erode. The legal and ethical concerns surrounding AI in criminal justice are extensive and multifaceted. From algorithmic bias and opacity to accountability gaps and privacy risks, these challenges underscore the need for cautious and critical adoption. Left unaddressed, such issues could undermine fundamental rights, entrench systemic discrimination, and weaken public confidence in justice systems. Acknowledging these risks is a crucial step toward designing legal and regulatory frameworks that mitigate harms while preserving the potential benefits of AI.

5. Adequacy of Existing Legal Frameworks

5.5 Nigerian Constitutional and Judicial Approaches

Nigeria's 1999 Constitution (as amended) provides a robust foundation for rights protection, though its application to AI in criminal justice remains underdeveloped. Two provisions are particularly relevant:

- **Section 36** guarantees the right to fair hearing within a reasonable time before a competent court. This principle is vital when considering algorithmic decision-making in bail, sentencing, or parole, since opaque or biased AI systems could undermine due process.
- **Section 37** protects the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. This provision is directly relevant to AI surveillance, biometric collection, and data-driven policing.

Nigerian courts have interpreted these rights in cases involving digital privacy and due process, offering insights into how they might extend to AI regulation:

1. **Digital Rights Lawyers Initiative v. National Identity Management Commission (NIMC)** (2021, Suit No. FHC/ABJ/CS/79/2020).
   The Federal High Court held that compelling Nigerians to provide National Identification Numbers without robust data protection mechanisms violated the constitutional right to privacy under Section 37. This precedent suggests that AI systems dependent on biometric or personal data must be accompanied by strong legal safeguards.
2. **Ubani v. Director, SSS** (1999) 11 NWLR (Pt. 625) 129.
   The Court of Appeal stressed that fair hearing under Section 36 is sacrosanct. Applied to AI, this implies that reliance on opaque algorithms in criminal proceedings could breach constitutional guarantees if defendants cannot challenge or understand the basis of algorithmic decisions.

3. **Emerging Markets Telecommunication Services Ltd. (EMTS) v. Barrister Godfrey Nya Eneye** (2018) LPELR-46189(CA).
   The Court of Appeal ruled that unauthorized disclosure of subscriber data infringed Section 37 privacy rights. This reinforces that state use of telecom or digital data for AI-driven surveillance must comply with privacy protections.
4. **Okafor v. Lagos State Government** (2016, High Court of Lagos State, unreported).
   The court invalidated indiscriminate data collection by government agencies, emphasizing the supremacy of individual rights over administrative convenience. This judgment signals judicial willingness to limit state power in digital governance contexts, a principle equally applicable to AI adoption.

Despite these advances, Nigeria faces significant **regulatory gaps**. The recently enacted **Nigeria Data Protection Act (NDPA), 2023** provides a statutory framework for personal data handling, but it is largely modelled on general data protection principles and does not address the specific risks of AI, such as algorithmic bias or automated decision-making in criminal justice. Enforcement capacity also remains limited due to resource constraints and institutional weaknesses. Thus, while Nigeria's constitutional provisions and emerging jurisprudence establish important protections, they remain reactive and fragmented. There is no comprehensive legal or policy framework dedicated to governing AI use in criminal justice. Without proactive regulation, Nigeria risks adopting AI technologies that undermine, rather than strengthen, con6. Towards Stronger Legal Safeguards

The preceding analysis shows that while existing legal frameworks—both international and domestic—offer some protection against risks associated with Artificial Intelligence (AI) in criminal justice, they are inadequate in their current form. Nigeria provides a useful case study for identifying both the opportunities and the gaps in legal protections, especially when compared with global developments. This section outlines key reforms and safeguards necessary to ensure that AI enhances, rather than undermines, justice.

6.1 Strengthening the Nigeria Data Protection Act, 2023

The enactment of the Nigeria Data Protection Act (NDPA), 2023 marked a significant step toward regulating data-driven technologies. However, the Act is largely modelled on general data protection principles and does not directly address AI-specific risks. For example, unlike the European Union's GDPR, the NDPA does not contain provisions equivalent to **Article 22 GDPR**, which grants individuals the right not to be subject to decisions based solely on automated processing.

Proposed Reforms:

- Amend the NDPA to introduce explicit protections against harmful automated decision-making in criminal justice.
- Establish a mandatory **"human-in-the-loop" requirement**, ensuring that algorithmic outputs in bail, sentencing, or parole cannot be determinative without judicial oversight.
- Create enforceable obligations for transparency, requiring law enforcement agencies to disclose the use of AI tools in investigations and trials.

6.2 Embedding Fair Hearing and Due Process Principles

Section 36 of the Nigerian Constitution guarantees fair hearing, but this right is threatened by the opacity of AI algorithms. Comparative experience shows that courts are beginning to grapple with this problem. In the U.S. case *State v. Loomis* (2016), concerns arose about reliance on the COMPAS tool in sentencing. Similarly, Nigerian courts may soon face challenges where defendants contest decisions influenced by opaque algorithms.

Proposed Reforms:

- Judicial recognition that algorithmic opacity is inconsistent with Section 36's fair hearing requirement.
- Issuance of **Practice Directions** by the Chief Justice of Nigeria mandating disclosure of AI tools used in criminal proceedings.
- Development of evidentiary standards requiring parties relying on AI-generated outputs to establish their scientific reliability and potential biases, mirroring the **Daubert standard** in the U.S.

6.3 Safeguarding Privacy Against AI Surveillance

Section 37 of the Constitution and jurisprudence such as *Digital Rights Lawyers Initiative v. NIMC* (2021) confirm privacy as a fundamental right. However, the expansion of AI-enabled surveillance—such as facial recognition and predictive policing—poses new challenges. The UK case *Bridges v. South Wales Police* (2020) illustrates how courts can apply privacy rights to regulate AI surveillance. Nigeria, too, must develop proactive safeguards.

Proposed Reforms:

- Enact statutory restrictions on the use of facial recognition technologies, modelled on the cautious approach taken in parts of the EU.
- Require independent judicial authorization before law enforcement can deploy AI surveillance tools.
- Establish oversight bodies with powers to audit law enforcement agencies for compliance with privacy rights.

6.4 Ensuring Accountability and Preventing Bias

One of the greatest risks of AI in criminal justice is the reproduction of societal biases. Studies in the U.S. have shown that risk-assessment algorithms disproportionately classify racial minorities as high-risk. Nigeria, with its ethnic and religious diversity, faces a similar danger. Without safeguards, AI could entrench discriminatory practices contrary to Section 42 of the Constitution, which prohibits discrimination.

Proposed Reforms:

- Mandate **algorithmic impact assessments** prior to deployment of AI in criminal justice.
- Introduce anti-discrimination provisions requiring developers and state agencies to test AI systems for bias before use.
- Create clear avenues for redress where individuals allege discrimination resulting from AI-driven decisions.

6.5 Institutional and Capacity-Building Measures

Even with strong laws, effective enforcement depends on institutional capacity. Nigeria faces challenges in this regard, including limited judicial expertise in emerging technologies and weak enforcement mechanisms within data protection authorities. By contrast, the EU complements regulation with independent supervisory authorities that monitor compliance.

Proposed Reforms:

- Establish a Specialized Technology and Law Unit within the judiciary to build expertise in handling AI-related disputes.
- Strengthen the Nigeria Data Protection Commission by granting it broader powers to audit, sanction, and guide law enforcement agencies deploying AI.
- Promote capacity-building programs for judges, lawyers, and law enforcement officials on AI ethics and law.

6.6 International and Regional Cooperation

AI governance is not a purely domestic issue. Nigeria's participation in international and regional initiatives will be critical to harmonizing standards and preventing regulatory arbitrage. For instance, the African Union's Data Policy Framework (2022) encourages member states to adopt rights-based approaches to data governance, though implementation remains uneven.

Proposed Reforms:

- Nigeria should champion an African Charter on AI and Human Rights, modelled after the EU's AI Act, but tailored to Africa's socio-legal context.
- Strengthen collaboration with regional bodies such as ECOWAS to develop common standards for AI use in criminal justice.
- Engage with international partners to adopt best practices on algorithmic transparency and accountability.

6.7 Summary of Reform Priorities

These risks illustrate that, without reform, AI could undermine rather than strengthen Nigeria's justice system. Situating Nigeria within international governance frameworks underscores the urgency of reform. The UN Guiding Principles on Business and Human Rights (UNGPs, 2011) require states to protect against human rights abuses linked to business activity, including technology companies supplying AI tools to law enforcement. Similarly, the OECD AI Principles (2019) call for AI systems that are transparent, fair, accountable, and respectful of human rights. The UNESCO Recommendation on the Ethics of AI (2021) further emphasizes inclusivity, non-discrimination, and human oversight as global standards for ethical AI deployment.

While Nigeria's Data Protection Act (NDPA) 2023 takes an important first step by restricting fully automated decision-making, it falls short of these international norms. Weak enforcement capacity, limited judicial oversight, and a lack of transparency obligations leave significant

gaps. In contrast, recent instruments such as the EU AI Act (2024) mandate bias testing, disclosure of high-risk systems, and independent monitoring. Aligning Nigerian reforms with such international best practices would help ensure that AI adoption strengthens, rather than erodes, the rule of law.

Reform Priorities for Nigeria

In summary, Nigeria's legal system requires a multi-pronged reform strategy to address the risks of AI in criminal justice:

- **Amend the NDPA 2023** to explicitly regulate automated decision-making in the justice sector.
- **Guarantee human oversight** in all AI-influenced criminal justice decisions.
- **Protect fair hearing rights** by mandating disclosure of AI tools' logic and reliability testing before deployment.
- **Restrict AI surveillance** to cases authorized by independent judicial oversight.
- **Prevent algorithmic bias** through mandatory human rights and impact assessments.
- **Build judicial and institutional capacity** to evaluate and govern AI systems.
- **Promote regional and international cooperation** to align Nigerian practices with global principles, including the UNGPs, OECD AI Principles, and UNESCO standards.

By embedding these safeguards, Nigeria can balance the benefits of AI in crime prevention and justice administration with the protection of human rights, social equity, and public trust.

7. Conclusion and recommendation

The integration of Artificial Intelligence (AI) into criminal justice systems represents both a transformative opportunity and a significant risk. As this paper has demonstrated, AI tools—ranging from predictive policing and risk assessment algorithms to biometric surveillance—have the potential to improve efficiency, enhance decision-making, and support evidence-based interventions. However, their deployment also raises serious concerns regarding transparency, accountability, privacy, and fairness. If left unregulated, AI may entrench systemic inequalities, undermine due process, and erode public trust in the rule of law.

Nigeria provides a compelling case study in this regard. While the 1999 Constitution guarantees fundamental rights such as fair hearing (Section 36) and privacy (Section 37), and the Nigeria Data Protection Act (NDPA) 2023 has begun to address issues of data governance, the current framework remains inadequate to manage AI-specific risks. Automated decision-making, algorithmic bias, and opaque surveillance practices present unique threats that require more targeted safeguards. Comparative insights from jurisdictions such as the United States, the United Kingdom, India, and particularly the European Union—with its Artificial Intelligence Act (2024)—illustrate that even advanced legal systems are grappling with similar challenges. For Nigeria, the lesson is clear: reform must come before AI becomes deeply embedded in its criminal justice system without proper oversight.

To address these challenges, Nigeria should pursue a comprehensive reform agenda that combines legal innovation, judicial vigilance, institutional strengthening, and international collaboration. The following policy recommendations summarize the core priorities identified in this study:

- **Legislative Reform:** Amend the NDPA 2023 to explicitly regulate automated decision-making, mandate human oversight, and require transparency in the deployment of AI within criminal justice.
- **Judicial Oversight:** Develop practice directions and evidentiary standards to ensure that AI technologies do not compromise the constitutional right to a fair hearing.
- **Privacy Protections:** Restrict AI-driven surveillance to cases authorized by independent judicial approval, in line with constitutional guarantees of privacy.
- **Bias Prevention:** Introduce mandatory algorithmic impact assessments and anti-discrimination audits prior to deploying AI in law enforcement or judicial processes.
- **Institutional Strengthening:** Invest in the capacity of courts, regulators, and oversight bodies to evaluate AI systems and enforce compliance with rights-based standards.
- **Regional and International Cooperation:** Engage actively in African Union initiatives and align national frameworks with global instruments such as the UN Guiding Principles on Business and Human Rights (2011), the OECD AI Principles (2019), and the UNESCO Recommendation on the Ethics of AI (2021).

In conclusion, the challenge for Nigeria—and indeed for the global community is to strike a careful balance between harnessing the benefits of AI and safeguarding fundamental rights. Achieving this balance requires foresight, strong institutions, and alignment with international norms. By adopting proactive reforms, Nigeria can protect its citizens from the risks of AI-driven criminal justice while positioning itself as a leader in rights-based AI governance across Africa.

References

- Akinola, A. O. (2020). Ethnic profiling and policing in Nigeria: Implications for human rights and justice. *African Security Review, 29*(3), 273–290.
- Amnesty International. (2020). *Nigeria: Authorities must end impunity for police violence in wake of #EndSARS protests.* Retrieved from https://www.amnesty.org
- Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). *Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks.* ProPublica.
- Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review, 104*(3), 671–732.
- Bridges v. South Wales Police [2020] EWCA Civ 1058 (UK Court of Appeal).
- Bryson, J. (2020). The past decade and future of AI's impact on society. In M. C. Horowitz (Ed.), *AI and International Affairs.* Brookings Institution Press.
- Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence.* Yale University Press.

- Digital Rights Lawyers Initiative v. National Identity Management Commission (NIMC), Suit No. FHC/ABJ/CS/79/2020 (Federal High Court, Nigeria).
- Emergent Markets Telecommunication Services Ltd. v. Eneye (2018) LPELR-46189(CA) (Court of Appeal, Nigeria).
- European Commission. (2024). *The EU AI Act enters into force.* Brussels: European Union. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- European Union. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act).* COM/2021/206 final.
- Federal Republic of Nigeria. (2023). *Nigeria Data Protection Act (NDPA).* Official Gazette, Abuja.
- Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement.* NYU Press.
- General Data Protection Regulation, Regulation (EU) 2016/679.
- Human Rights Watch (HRW). (2020). *Nigeria: Events of 2020. World Report 2021.* Retrieved from https://www.hrw.org
- Lum, K., & Isaac, W. (2016). To predict and serve? *Significance, 13*(5), 14–19.
- OECD. (2019). *OECD Principles on Artificial Intelligence.* Paris: OECD.
- Okafor v. Lagos State Government (2016) (High Court of Lagos State, unreported).
- Okagbue, I. (2021). Justice sector reforms in Nigeria: Challenges and prospects. *Journal of African Law, 65*(1), 87–105.
- State v. Loomis, 881 N.W.2d 749 (Wis. 2016) (Supreme Court of Wisconsin, USA).
- ThisDayLive. (2025, May 3). *Addressing data privacy concerns in artificial intelligence systems: Regulatory mechanisms in Nigeria.* Retrieved from https://www.thisdaylive.com
- Ubani v. Director, SSS (1999) 11 NWLR (Pt. 625) 129 (Court of Appeal, Nigeria).
- UNESCO. (2021). *Recommendation on the Ethics of Artificial Intelligence.* Paris: UNESCO.
- UNESCO. (2025, February 29). *Harnessing AI for justice: Balancing innovation and equity in East Africa.* Retrieved from https://www.unesco.org/en/articles/harnessing-ai-justice-balancing-innovation-and-equity-east-africa
- United Nations. (2011). *Guiding Principles on Business and Human Rights.* Geneva: United Nations.