



Evaluating the Role of Facial Recognition Technology in Crime Prevention and Law Enforcement in Nigeria

Oladejo, A. O. and Alabi R. A.

Department of Sociological Studies, Tai Solarin Federal University of Education, P.M.B 2118, Ijebu-Ode, Ogun State, Nigeria

Corresponding email: ayooladejo23@gmail.com

Abstract

The use of facial recognition technology at airports and in criminal investigations has made facial recognition technology (F.R.T), fast becoming a potent tool in Nigerian law enforcement. Using three disciplinary lenses, sociology, law, and criminology, this study critically assesses FRT's potential for crime prevention in Nigeria. Sociologically speaking, FRT runs the risk of normalising monitoring, strengthening social inequality through skewed misidentifications, and undermining institutional trust, which is already brittle. By designating biometric identifiers as sensitive data and mandating proportionality, monitoring, and remedies, Nigeria's Data Protection Act 2023 represents a significant legal advancement. However, there are still serious issues with operational rules, training, and enforcement. In terms of criminology, FRT provides investigative advantages including expedited suspect identification and evidence support; however, they are counterbalanced by the significant of falsehood. Similar conflicts are highlighted by comparative data from other jurisdictions, underscoring the need to strike a balance between the promise of technology and the dangers of human rights abuses and declining police legitimacy. Premature or widespread deployment is particularly troublesome in Nigeria due to the country's inherent security issues, poor public confidence, and lax regulatory enforcement. Narrowly specified legal authorisations, human oversight, required effect assessments, capacity building, and phased deployment are all suggested in the article's conclusion. Ultimately, whether FRT is incorporated into robust protections that uphold justice, accountability, and democratic governance will determine its success in Nigeria more than its technical complexity.

Keywords: Nigeria, biometric, law enforcement, crime prevention, and facial recognition technologies.

1. Introduction

Biometric technologies have grown more and more integrated into states' security and governance frameworks in the twenty-first century. Among these, facial recognition technology (FRT) has garnered special interest due to its potential to revolutionise both criminal investigation and individual identification. FRT presents special ethical and legal issues; unlike fingerprint or iris scans, it can be utilised passively, often without people's knowledge, through mobile devices and surveillance cameras (Raji & Buolamwini, 2023). Interest in FRT is rising quickly in Nigeria. In collaboration with technology companies like NEC, the federal government has tested face recognition technology at major international airports in Abuja and Lagos with the purported goal of enhancing border control and aviation security (Biometric Update, 2023).

In order to improve criminal investigation through automated suspect identification, Nigerian academics have also created prototype systems, such as the Digital Criminal Biometric Archives and Facial

Recognition System (DICA-FRS) (Ndubuisi et al., 2024). These projects show a strong technological and policy desire to include biometrics in law enforcement. Evidence from other jurisdictions, however, shows conflicting findings. For example, in the United States, Amnesty International (2021) cautioned that such technologies frequently exacerbate racial inequality in policing, also stringent restrictions and human control have been made by the World Economic Forum and INTERPOL (2022), stating that FRT should only be used for specific law enforcement investigations and not for indiscriminate public surveillance.

The appeal of FRT is evident in Nigeria, where law enforcement must contend with organised crime, terrorism, kidnapping, and cyber-enabled fraud. Although FRT may result in erroneous arrests, invasions of privacy, and a decline in public confidence in security agencies, if it is not properly governed. Therefore, this article assesses FRT in Nigeria from three disciplinary angles: criminology, which assesses the technology's efficacy, deterrent potential, and risks of miscarriages of justice; sociology, which investigates how surveillance alters state-citizen relations and social trust; and law, which looks at the implications for Nigeria's data-protection regime and constitutional rights.

Oladejo, A. O., & Alabi, R. A. (2025). Evaluating the Role of Facial Recognition Technology in Crime Prevention and Law Enforcement in Nigeria. *The Vocational and Applied Science Journal (VAS)*, vol. 19, no. 1, pp. 21-26.

©COVTEd Vol. 19, No. 1, Nov 2025

2. Scope of the Analysis

2.1 Relevance to Nigeria

Publications discussing Nigerian experiences were given priority, including Nigerian prototypes like the DICA-FRS system (Ndubuisi et al., 2024) and the government's FRT pilots at airports (Biometric Update, 2023). The analysis relied heavily on legal commentary on Nigeria's changing data protection laws, including the 2019 Nigeria Data Protection Regulation (NDPR), the Data Protection Bill (PwC, 2020), and the 2023 Nigeria Data Protection Act (Future of Privacy Forum, 2023; ICLG, 2025).

2.2 Comparative Insights

To offer lessons relevant to Nigeria, international reports and critiques were incorporated. Comparative benchmarks were offered, for instance, by the INTERPOL/World Economic Forum's (2022) framework for responsible usage in law enforcement, Amnesty International's (2021) campaign exposing racial bias, and the U.S. GAO's (2023) study on government use of FRT.

2.3 Credibility and Decency

Sources from 2020 to 2025 were chosen to represent the state of governance, scholarly discussions, and technology capabilities. This made sure that rather than discussing earlier, less advanced phases of biometric use, the research focused on Nigeria's current policy moment. Three disciplinary lenses are integrated into the analytical framework:

- a) Social: investigating how FRT affects social inequality, institutional legitimacy, and surveillance culture (Amnesty International, 2021; Raji & Buolamwini, 2023).
- b) Legal: checking for adherence to Nigeria's NDPA and constitutional norms, such as those about human oversight, proportionality, and remedies (PwC, 2020; Future of Privacy Forum, 2023; ICLG, 2025).
- c) Criminal: determining whether FRT improves detection, deterrence, and the strength of the evidence, or if the hazards are more than the advantages (Ndubuisi et al., 2024; GAO, 2023; Taliaferro, 2025).

3. Nigerian Developments and the International Policy Landscape

Nigeria has seen the rise of facial recognition technology (FRT) in the face of increased security threats, such as organised crime, banditry, terrorism, and cyber-enabled crimes. Through the integration of digital technologies, the Nigerian government has attempted to update its policing infrastructure in recent years. The announcement and implementation of FRT systems at the Murtala Muhammed International Airport in Lagos and the Nnamdi Azikiwe International Airport in Abuja in 2023, in collaboration with NEC Corporation, was one obvious step (Biometric Update, 2023). Strengthening border security, thwarting identity theft, and expediting passenger screening were the declared goals. Parallel to these

policy moves, Nigerian scholars have advanced prototype innovations, such as the Digital Criminal Biometric Archives and Facial Recognition System (DICA-FRS), designed to automate the matching of suspect images with criminal databases using Haar cascades classifiers (Ndubuisi et al., 2024). While still experimental, these initiatives illustrate a domestic recognition of the investigative potential of FRT.

Multistakeholder efforts, on the other hand, have attempted to find a middle ground. A framework for "responsible limits" on FRT was proposed by the World Economic Forum and INTERPOL in 2022. It suggests using FRT exclusively for certain investigation goals that are backed by human oversight and open accountability systems. This methodology applies to Nigeria, where unchecked biometric surveillance is especially troublesome due to state capacity limitations and poor public trust in law enforcement. All things considered, Nigeria is at a crossroads: although legislative frameworks and technical capability are developing, global data emphasises that the hasty or widespread implementation of FRT can exacerbate already-existing disparities, erode legitimacy, and spark public opposition.

3.1. The Sociological Perspectives

Sociologically speaking, FRT is a social practice that alters power dynamics, institutional legitimacy, and people's lived experiences rather than just being a technological instrument. Three related themes are used in the following subsections to examine their consequences in Nigeria.

3.1.1 Surveillance, Normalisation and Chilling Effect

The focus of surveillance studies is on how technologies get ingrained in daily social life when they are implemented. Installing FRT in public areas like stadiums, airports, or transit hubs runs the potential of fostering a culture of continuous surveillance where people modify their behaviour because they believe they are always being observed (Amnesty International, 2021). Particularly in situations when freedom of expression is already precarious, such "chilling effects" have the potential to stifle acceptable civic engagements, such as political protest and public assembly.

The implementation of widespread FRT may increase concerns of retaliation or profiling in Nigeria, where protests against police misbehaviour, most notably the #EndSARS protests, have brought attention to tensions between the populace and security forces. There is a chance that monitoring technology may be seen as an extension of the state's coercive power rather than as neutral. According to sociology, the normalisation of biometric surveillance may, therefore, result in a decline in civic participation and a decreased desire to work with law enforcement, defeating the objectives of crime prevention.

3.1.2 Social Sorting and Unequal Visibility

The concept of "social sorting," in which certain groups are disproportionately impacted by technologies more than others, is another major worry. Studies reveal that a large number of commercial FRT algorithms have increased error rates in recognising women, younger individuals, and people with darker skin tones (Raji & Buolamwini, 2023). Similar to this, Aboujaoude et al. (2023) note that bias, misidentification, and the moral use of private biometric information are ongoing worries regarding facial recognition systems. The risk of demographic bias is especially significant for Nigeria, a multiethnic country with a wide range of phenotypic characteristics. Due to algorithmic misclassifications, communities who are already overpoliced, such young urban males, may be even more vulnerable to erroneous suspicion or arrest. The perception that monitoring is not used consistently and instead targets particular groups is strengthened by this unequal visibility, which further exacerbates social hierarchies and marginalisation. According to sociological theory, FRT might serve more as a selective control mechanism than as a general security instrument.

3.1.3 Institutional Trust and Police Legitimacy

Nigerian policing has long suffered from a lack of public trust brought on by ideas of violence, corruption, and ineptitude. Since community collaboration through reporting, intelligence sharing, and compliance depends on whether or not people believe that police are just and accountable, law enforcement legitimacy is vital. This tenuous credibility could be undermined by the implementation of FRT without sufficient protections. The public's trust in law enforcement agencies may further erode if they believe that FRT is applied arbitrarily or opaquely. Public confidence necessitates the limited, supervised, and accountable use of biometric technologies, as the World Economic Forum and INTERPOL (2022) highlight. Sociologically speaking, this is consistent with the theory of procedural justice, which emphasises that legitimacy depends more on perceptions of fairness and transparency than just crime-control results. Therefore, Nigeria faces two challenges: first, ensuring FRT is fair, accurate, and compliance with the law; and second, making sure the public is aware of the extent, protections, and redress procedures that are in place. Without these steps, FRT runs the potential of not being a tool for creating safer communities but rather another representation of state overreach.

3.2 The Legal Perspective.

Classifying biometric data must be the first step in any legal examination of FRT in Nigeria, but it cannot stop there. Equal consideration must be given to broader issues about human oversight, automated decision-making, and redress for individuals who are negatively impacted.

3.2.1 Biometric Data as Sensitive Data

A major step towards elucidating the legal handling of biometric identifiers is the Nigeria Data Protection Act (NDPA) of 2023. It clearly classifies biometric information, such as facial photos used for identification, as "sensitive personal data," which calls for stronger protections and more stringent requirements for processing that is permitted by law (Future of Privacy Forum, 2023; ICLG, 2025). Before gathering or using such data, law enforcement organisations must show need, proportionality, and a clear legal basis under this framework.

Nigeria is now in compliance with international norms, such as the General Data Protection Regulation (GDPR) of the EU, which likewise considers biometric information to be sensitive. The focus on proportionality is especially pertinent to policing contexts: while FRT may be used for specific, serious-crime investigations, widespread surveillance in public areas may violate the NDPA. Thus, the Act gives Nigerian courts a starting point for examining whether the use of FRT complies with the right to privacy guaranteed by the 1999 Constitution (Section 37 as amended).

3.2.2 Automated Decision-Making and Oversight

The danger of automated decision-making without sufficient human monitoring is one of the most hotly debated topics in FRT governance. The risks of treating algorithmic results as conclusive proof instead of investigative leads are highlighted by global experience (GAO, 2023; Amnesty International, 2021). Racial minorities have been disproportionately affected by misidentifications that have resulted in unjust arrests in the US, highlighting the dangers of relying too heavily on machine outputs.

There may be a strong temptation to delegate decision-making to automated systems in Nigeria, where law enforcement agencies frequently struggle with a lack of funding and technical know-how. However, the NDPA stipulates that major decisions that influence individuals cannot be made entirely by automated processing without meaningful human review, and it requires impact assessments for high-risk processing activities, such as biometric surveillance (ICLG, 2025). This establishes a legal requirement to incorporate human oversight into the process of conducting investigations.

3.2.3 Training, Policies and Remedies

Statutes alone are not enough to ensure legal conformity; operationalisation through policies and training is also essential. Federal agencies were chastised by the U.S. GAO (2023) for having no documented policies for the use of FRT, which led to inconsistent practices and possible rights violations. There is a comparable risk in Nigeria, where internal policies regarding biometric surveillance and police training programs are still in their infancy. The Nigeria Data Protection Commission can receive complaints

under the NDPA, which offers remedies. However, accessible redress for those falsely accused or surveilled must be part of the remedies, which must extend beyond regulatory fines. This could entail institutional accountability for abuse as well as judicial review of police use of FRT material. Legal protections are only effective if they are available to regular people, especially those who are most at risk from surveillance.

3.3 The Criminological Perspectives.

The crucial question in criminology is not merely whether FRT can identify specific people, but also if it enhances justice results without causing undue harm. This section examines the usefulness of investigations, error hazards, and the ambiguous deterrent effects of monitoring.

3.3.1 Investigative Utility and Evidentiary Value

FRT's proponents contend that by expediting the identification of suspects, finding missing people, and connecting offenders across several events, it improves law enforcement's ability to carry out its duties. Experimental systems such as DICA-FRS (Ndubuisi et al., 2024) demonstrate how automated facial matching can support criminal investigations in Nigeria. When combined with other types of evidence, FRT may further increase the evidential value by offering support for prosecutors' choices. Globally, FRT has been approved by INTERPOL and the World Economic Forum (2022) as a potentially useful investigative tool, as long as its application is limited to specific and appropriate purposes. The criminological justification is that FRT may increase criminal clearance rates by decreasing investigative lag periods and enhancing suspect identification accuracy.

3.3.2 Errors, False Positives and Wrongful Outcomes

However, there are also serious concerns, according to criminological studies. FRT system errors, especially false positives, can result in miscarriages of justice, squandered investigative resources, and erroneous arrests. According to studies, women and people with darker skin tones are disproportionately affected by mistake rates, which are not spread evenly (Raji & Buolamwini, 2023). These mistakes could result in actual damages like arbitrary incarceration and reputational harm in places like Nigeria where procedural safeguards are lax. According to Aboujaoude et al. (2023), FRT presents significant moral dilemmas pertaining to responsibility and fairness, particularly when algorithmic conclusions are opaque. The primary focus of criminology is not only accuracy but also the consequences of incorrect identifications on the criminal justice system and public confidence in law enforcement.

3.3.3 Deterrence: Uncertain Impacts

The possible deterrent impact of FRT the notion that widespread surveillance deters criminal activity is another argument put up in favour of it. However,

whether surveillance technologies truly reduce crime or just replace it is still up for debate in criminological study. While Amnesty International (2021) warns that continuous surveillance can inhibit lawful conduct without necessarily stopping determined offenders from acting, Taliaferro (2025) points out that FRT may promote national security by limiting anonymity.

The deterrent power of FRT is probably limited in Nigeria, where structural reasons like unemployment, poverty, and poor enforcement institutions are major contributors to many crimes. In reality, according to criminological theory, the more important deterrent is the certainty of punishment rather than the mere awareness of surveillance. The installation of FRT cameras might not significantly lower crime rates on its own unless there are changes made to institutional legitimacy, judicial efficiency, and investigative follow-through.

4. Benefits and Risks Synthesised

A multidisciplinary assessment of facial recognition technology (FRT) in Nigeria reveals a nuanced interaction between advantages and disadvantages that defies easy categorisation.

4.1 Potential Benefits

According to criminology, FRT can help find missing people, identify suspects more quickly, and validate investigation leads (Ndubuisi et al., 2024; World Economic Forum & INTERPOL, 2022). As tested in airports in Abuja and Lagos, its incorporation into border control shows promise in thwarting identity theft and enhancing aviation security (Biometric Update, 2023). Legally, the Nigeria Data Protection Act 2023's designation of biometric data as sensitive offers a formal framework for preventing abuse while maintaining proportionality (Future of Privacy Forum, 2023; ICLG, 2025). Sociologically speaking, FRT could strengthen the idea that law enforcement is technologically savvy and capable of defending the public by enhancing perceptions of state capacity provided it is implemented fairly and transparently.

(1) Risks and Harms: Yet these benefits are tempered by substantial risks. Marginalised groups may be disproportionately affected by wrongful arrests caused by errors in algorithmic outputs (Raji & Buolamwini, 2023; Aboujaoude et al., 2023). Sociologically speaking, the normalisation of widespread surveillance could have chilling consequences that discourage legitimate civic participation, especially in politically delicate situations (Amnesty International, 2021). Legally speaking, there is a chance that due process and privacy rights under the constitution will be violated, especially if automated decision-making takes place without adequate human monitoring (GAO, 2023). According to criminology, FRT's deterrent effect is yet unknown, and its implementation might not result in appreciable drops in crime rates until systemic changes are made to the legal and investigative systems (Taliaferro, 2025).

(2) Synthesis: Thus, a conflict between the promise of technology and the socio-legal reality arises. Nigeria stands to gain from FRT if it is carefully circumscribed, targeted, and embedded within robust legal, ethical, and institutional safeguards. However, in the absence of these circumstances, the dangers of selective enforcement, rights breaches, and deteriorating police legitimacy might outweigh any possible advantages.

5. Policy Recommendations.

Several policy suggestions for Nigeria's use of FRT in crime prevention can be made based on the interdisciplinary analysis:

(1) Narrow and Specific Legal Authorisation: Nigerian legislation ought to clearly outline the situations in which FRT might be used, such as for border security, terrorist investigations, and major crime investigations, while outlawing its careless application in public areas. This would protect constitutional rights and guarantee adherence to the NDPA's proportionality principle (Future of Privacy Forum, 2023; ICLG, 2025).

(2) Mandatory Impact Assessments: As mandated by the NDPA, law enforcement organisations must perform Data Protection Impact Assessments before implementing FRT. To guarantee openness and public accountability, these evaluations must be made public, outlining potential hazards, precautions, and oversight procedures.

(3) Human Oversight and Accountability: Decisions made automatically should never be final. FRT results should not be regarded as definitive proof, but rather as research leads. In order to identify abuse or bias, clear policies should be subject to human assessment at every stage, backed by independent auditing (GAO, 2023).

(4) Technical Accuracy and Bias Mitigation: It should be mandatory for vendors providing FRT to Nigerian authorities to release reports on their accuracy and demographic performance. Systems should limit false positives across age, gender, and ethnic groups, according to independent testing (Raji & Buolamwini, 2023).

(5) Capacity Building and Training: Strong training is necessary for Nigerian police and security personnel in the ethical, legal, and evidential norms governing biometric evidence in addition to the technical application of FRT. The GAO's (2023) report on U.S. agencies provides valuable insights into the dangers of insufficient policy frameworks.

(6) Accessible Remedies for Citizens: People who feel they have been wrongfully identified or improperly the target of surveillance must have easy access to channels for recourse, such as court review and complaints to the Data Protection Commission.

Remedies should be affordable, accessible, and enforceable to strengthen trust.

(7) Public Communication and Engagement: For policing to be legitimate, trust is essential. Authorities should discuss the scope and protections of FRT with community stakeholders, academics, and civil society. Open communication can boost public trust and allay concerns about indiscriminate surveillance (Amnesty International, 2021).

(8) Incremental Deployment with Evaluation: Nigeria should implement FRT in stages rather than all at once, starting with controlled settings like airports or high-security facilities. Before expanding, each stage should be independently assessed for efficacy, legality, and social impact.

6. Limitations and Research Agenda.

A number of limitations should be noted, even though this study provides a critical, multidisciplinary assessment of face recognition technology (FRT) in Nigeria.

First, based on secondary data from reports, scholarly literature, and governmental papers, the study is mainly conceptual and normative. Empirical fieldwork on the operationalisation of FRT in law enforcement practice is lacking in Nigeria. For instance, although pilot deployments at airports have been reported (Biometric Update, 2023), there are no independent assessments of their efficacy, mistake rates, or public opinion.

Second, the sociopolitical environment of Nigeria has particular difficulties, like lax enforcement of laws. Comparative international literature does not adequately address resource constraints and public mistrust of law enforcement. Lessons from Europe (Amnesty International, 2021; Raji & Buolamwini, 2023) and the United States (GAO, 2023) are illuminating, although they might not directly apply to Nigeria's institutional realities.

Third, the author hasn't thoroughly examined how FRT interacts with other cutting-edge technologies like integrated national identity systems, mobile data analytics, and predictive policing powered by AI. These connections may increase dangers or create new channels for responsibility.

7. Conclusion

Facial recognition technology (FRT) in Nigerian law enforcement has been critically assessed in this paper from criminological, legal, and social angles. It concludes that although FRT has a great deal of promise to improve the effectiveness of investigations, fortify border security, and aid evidential procedures, these advantages are outweighed by serious concerns. These include threats to the constitutional rights to privacy and due process, algorithmic prejudice, false positives that result in erroneous arrests, and a chilling

effect on civic engagement.

With the Nigeria Data Protection Act 2023, which offers a framework for regulating sensitive biometric data, Nigeria has made significant legal advancements. However, the law runs the risk of staying aspirational in the absence of rigorous implementation, training, and easily available remedies. The technology's deterrent effect in criminology is still unclear, especially in light of the fact that structural factors that contribute to crime are still neglected. According to sociology, unrestricted surveillance may worsen the already shaky public confidence in law enforcement.

According to the synthesis of these viewpoints, Nigeria is at a turning point in its policymaking. If implemented gradually, openly, and under strict supervision, FRT may help achieve certain crime-prevention objectives. It runs the potential of escalating societal injustices, threatening police legitimacy, and violating fundamental rights if used carelessly or without accountability. A careful, evidence-based, and collaborative strategy is necessary for the future. To make sure that biometric innovation enhances rather than detracts from Nigeria's democracy and justice systems, legislators, law enforcement, technologists, and civil society must work together.

References

- Aboujaoude, E., Gega, L., & Parrish, M. B. (2023). Facial recognition and mental health: Ethical considerations. *World Psychiatry*, 22(2), 245–246. <https://doi.org/10.1002/wps.21089>
- Amnesty International. (2021). *Ban dangerous facial recognition technology that amplifies racist policing*. Amnesty International. <https://www.amnesty.org/en/latest/news/2021/01/ban-dangerous-facial-recognition-technology>
- Biometric Update. (2023, June 28). *Nigeria trials facial recognition system at airports with NEC, seeks vendors for further rollout*. <https://www.biometricupdate.com/202306/nigeria-trials-facial-recognition-system-at-airports>
- Future of Privacy Forum. (2023, June 13). *Nigeria enacts Data Protection Act, expanding on 2019 regulation*. Future of Privacy Forum. <https://fpf.org/blog/nigeria-enacts-data-protection-act>
- Government Accountability Office [GAO]. (2023). *Facial recognition technology: Federal use and related privacy concerns*. U.S. GAO. <https://www.gao.gov/products/gao-23-105189>
- ICLG. (2025). *Nigeria: Data protection laws and regulations 2025*. International Comparative Legal Guides. <https://iclg.com/practice-areas/dataprotection-laws-and-regulations/nigeria>
- Ndubuisi, C. I., Okezie, C. A., & Ogu, C. C. (2024). Development of a digital criminal biometric archives and facial recognition system for crime detection. *Nigerian Journal of Technology*, 43(1), 112–122. <https://doi.org/10.4314/njt.v43i1.12>
- PWC. (2020). *Nigeria Data Protection Bill 2020: Key highlights and implications*. Price water house Coopers Nigeria. <https://www.pwc.com/ng/en/assets/pdf/nigeria-data-protection-bill-2020.pdf>
- Raji, I. D., & Buolamwini, J. (2023). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. *Proceedings of the ACM on Human-Computer Interaction*, 7(CSC1), 1–29. <https://doi.org/10.1145/3579504>
- Taliaferro, C. (2025). Facial recognition technology and national security: Evaluating risks and opportunities. *Journal of Security Studies*, 48(2), 156–173. <https://doi.org/10.1093/jss/48.2.156>
- World Economic Forum & INTERPOL. (2022). *Responsible limits on facial recognition: The law enforcement assessment list*. WEF. https://www3.weforum.org/docs/WEF_Responsible_Facial_Recognition_2022.pdf