LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S4(2025)

ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATIONS IN SAUDI ARABIA: ADVANCEMENTS, CHALLENGES, AND A SHARIA-COMPLIANT FRAMEWORK

Fahad Abdullah Moafa[1], Hamad Salem Almarri[2]

[1]Assistant Professor, Department of Computer Science, King Fahad Naval Academy. Jubail, Saudi Arabia.
[2]Assistant Professor, Department of Law, College of Law, King Faisal University. Hofuf, Al-Ahsa, Saudi Arabia.

fah171393@hotmail.com[1]
halmarri@kfu.edu.sa[2]

Abstract
Technological modernization is one of the areas highlighted in the Vision 2030 of Saudi Arabia because it is a way to improve the level of public safety, so Artificial Intelligence (AI) is redefining criminal investigation. This article is exploring the transforming effects of artificial intelligence (AI) applications such as fraud detection, biometric identification, crime scene reconstruction, and a new reporting system of cyber harassment within the Saudi Arabian judicial and cultural ethos. With AI-based technology, there was a 90 % of identifying fraudulent transactions, SAR 2 billion saved and 60 % of 1, 200 cases identified the suspect in 2024. Nevertheless, some difficulties have to be clarified, including legal ambiguities in using evidence provided by AI, protecting of privacy rights as comprehended by the Personal Data Protection Law, and the emergence of algorithmic bias, which all requires a strong regulation field. An ethical example of such innovation concerns a proposed application using AI to combat cyber harassment in the Saudi culture. Ways forward will include the creation of a national AI regulatory body, incorporation of global standards, such as the European Union AI Act, and a Sharia compliant approach to counter technological efficiency with equity and societal confidence.

1. Introduction

Saudi Arabia has its own Vision 2030 plan, introduced in 2016, where economic diversification and modernization of public services are the priorities and public safety plays a pivotal role. The field of Artificial Intelligence (AI) is revolutionizing criminal investigation, and it is possible to quickly process large amounts of data and identify a person with high precision and automatize legal proceedings (AL samara& Ghazi, 2024). Applications of AI, e.g., fraud prevention or biometric identification, facilitate more efficient and more accurate work of law enforcement, which is in line with the policy of smart governance in Saudi Arabia. By 2024, AI solutions were noticing 90 % of the fraudulent transactions, saving the country SAR 2 billion, and identifying the guilty party in 60 % of cases out of 1,200 instances (Mohammed & Al-Abdul Rahman, 2024). Among them, an interesting case is an AI-driven cyber harassment reporting app with coded identifiers of victim confidentiality supposed to functionally respond to criminal cases such as a bullying situation or a defamation case based on the cultural and legal standards of the Saudi Kingdom (Moafa et al., 2018). The established improvements are aligned with the vision 2030 and its aim to place Saudi Arabia among the leading contenders in technology-based safety in public interventions.

Technical and legal ambivalence in Deployment of AI in Sharia-compliant justice system is however simplified by legal uncertainties, breaching of privacy based under the Personal Data Protection Law and algorithm bias that pose risks (Alshahrani et al., 2021). In 2024, 30 % of all cases of cybercrimes have been postponed because of the lack of clarity regarding the requirements of the admissibility of AI evidence (Latham & Watkins LLP, 2024). The ethical concerns regarding the aspect of biasness during facial recognition as a result of small Arabic dataset require frequent audits and culturally aware algorithms (Buolamwini & Gebru, 2020). In

this article, the researcher assesses the performance of AI in Saudi criminal investigation and recommends a customized framework, which includes establishing a national authority to oversee the use of AI, and Sharia-compatible guidelines that will not only provide ethical usage of AI, but also will bring about trust and impartiality to the court system.

2. AI Applications in Saudi Criminal Investigations

AI's integration into Saudi Arabia's criminal justice system spans multiple domains, each addressing specific investigative needs while advancing Vision 2030's technological goals.

2.1 Digital Evidence Analysis

The explosion in cybercrimes including electronic fraud and identity theft has pushed the old ways of investigation to the limit. Artificial intelligence (AI) software, such as Cellebrite (Universal Forensic Extraction Device) can extract and analyze data on smartphones and computers with an 85% success level in recovering evidence and can significantly decrease the efforts put into investigations (Casey, 2021). As an example, to handle terabytes of digital evidence in an hour in 2024, it took some time in weeks in the past (Horsman, 2020). In fraud in finance, AI algorithms monitor cloud-based transactions and identify 90 per cent of suspected transactions and save the Saudi banks SAR 2 billion every year (Mohammed & Al-Abdul Rahman, 2024). These systems allow the detection of patterns, which cannot be done manually, improving the efficiency of the investigations and increasing the success of digital transformation as outlined in Vision 2030.

2.2 Pattern Recognition and Analysis of Criminal Behavior

This skill of picking up trends in behavioral and transactional data is crucial in fighting complex crime such as money laundering where AI comes in very handy. Saudi Financial Intelligence Unit (SFIU) uses machine learning to monitor the suspicious transactions and reached 95 % precision in 2024 and detected SAR 1.5 billion of illicit outflows (FATF, 2024). Within the context of urban policing, predictive models powered by AI have been used to analyze crime data and thus map the hotspots where response times dropped by up to 20 % in Riyadh and Jeddah (Alshahrani et al., 2021). As an example, AI sets green or red flags to anomalous financial transfers as they occur so proactive policing more compatible with the aim of Saudi Arabia to have a safer society. Nevertheless, predictive models tend to induce bias, so regular audits are required to reduce biases and make the process of investigation fair (Berk, 2021). In the case of financial fraud, the AI algorithms process cloud-based transactions and uncover 90 % of the suspicious transactions and save the Saudi banks SAR 2 billion a year (Mohammed & Al-Abdul Rahman, 2024). Such systems detect sophisticated patterns, like illegal money movements that human decision-making can never detect, contributing to the digital transformation objectives of Vision 2030.

2.3 Biometric Identification

The use of facial and fingerprint recognition has strengthened the investigative efforts of Saudi Arabia. Integration with the facial recognition technology powered by AI allowed the Absher portal to drop the residency and visa fraud to 70 % in 2024 (Ng, 2024). In 60 % of 1,200 suspects, the Riyadh police used biometric databases and were 48 times more successful than in using multiple manual methods (AL samara& Ghazi, 2024). Fingerprint analysis in forensics laboratories with artificial intelligence was found to be 15 % more accurate than the conventional methods, which reduces the risk of human error when an operator gets tired (NIST, 2023). The Article 21 of the Personal Data Protection Law (PDPL) needs to be complied with in order to

address the privacy issues and to make sure the biometric information is ethically used (Crawford & Schultz, 2021).

2.4 Virtual Reality and 3D Modeling Based Crime Scene Reconstruction

The use of AI enabled 3D modeling and virtual reality (VR) to recreate a crime scene is transforming crime scene reconstruction in Saudi Arabia. Combining CCTV, laser, and photos readings, AI can produce accurate 3D models, resulting in 25 % higher clarity in the development of evidence reports (Smith, 2024). VR simulations were also used in a 2024 homicide case in Riyadh to explain to the judicial system the positioning of the perpetrator (AL samara& Ghazi, 2024). AI-driven reconstructions are interactive, unlike the original sketches; they minimize the impact of human error in courtrooms (Casey, 2021). The introduction of this approach faces limitations due to its prohibitive costs and requirement of special training, which requires an investment in capacity building (Horsman, 2020).

2.5 Smart Investigator Aids

Smart investigator aids based on Natural Language Processing (NLP), simplify case-management, including the summarization of Arabic-language case files and identification and prioritization of leads. Such systems lowered the workload of investigation by 25 % in the Saudi police departments in 2024 (Johnson, 2024). Saudi Anti-Corruption Authority (Nazaha) leveraged NLP to identify over SAR 500 million spent on fraudulent contracts that led to an increase in financial oversight by 30 % (ALQUAiZ, 2025). Real-time data can be found on sites such as Palantir Gotham, positively impacting the decision process in complex cases (Brayne, 2020). There is the significant role of human control to make sure that everything is transparent and complies with the principle of Sharia-compliant laws (Mansoor et al., 2024).

2.6 Case Study: AI-Based Cyber Harassment Reporting Application

An innovative use of AI software that involves dealing with cyber harassment has been suggested by Saudi research worker Fahad Abdullah Moafa because cyber harassment is a particularly relevant topic in Saudi Arabia (Moafa et al., 2018). The system is published in an International Journal of Engineering & Technology and they correspond with vision 2030 to enhance the vision related to the public safety and ethical usage of technology. The main characteristics of it are the following ones:

- ✓ Confidentiality: All the data of the victims is saved as coded identifiers, attributable to the National Information Center, and therefore the data is anonymous.
- ✓ Machine Processing: Cases are allotted codes through national ID or residency numbers and handled electronically so as to reduce human interference.
- ✓ Targeted Crimes: Includes sexual, racial, sectarian harassment, bullying, abuse at work and defamation crimes that contain the vulnerable e.g. domestic workers and children.
- ✓ Algorithmic Framework: N-gram, sentiment analysis algorithms paired with a lexicon dictionary to compare harassment words and find correlated legal cases to help judges use them in creating fair rulings.
- ✓ Implementation: It is accessible to use as a mobile or computer application that can be downloaded.

The pilot stage of the system in 2024 showed that it could minimize cyber harassment by 95 %, which would support the dignity of victims and combat the outside reporting of human rights abuse (Moala et al., 2018). The future stages will focus on electronically classifying crimes and suggest penalties in line with the Saudi laws and ensures efficiency of the court system without ignoring the Sharia.

3. Benefits of AI in Criminal Investigations

Artificial intelligence also referred to as (AI) in the kingdom of Saudi Arabia has transformed how criminal investigations are conducted in the country and has left behind some tremendous benefits that are consistent with the vision 2030 of forging a contemporary organizational system that can transform the justice system because it is activity driven and technology based. With the additional advantages of AI in respect of digital evidence examination, pattern identification, biometric recognition, and legal assistance, the law enforcement agencies in Saudi have been one of the most efficient, accurate, and analytically profound. These developments embrace the Kingdom desire to become the leader in smart governance by complying with the Sharia-compliant principles. Nevertheless, barriers, including the necessity to develop training and ethical supervision, have to be overcome in order to secure sustainable execution.

3.1 Increased speed and efficiency

AI greatly promotes investigations especially where it is related to cybercrimes whereby traditional ways are quite timely and resource intensive. Experience shows that digital evidence on smartphones and computers can be processed within hours, compared to weeks of manual work (Horsman, 2020) with the help of such tools as the Universal Forensic Extraction Device (UFED) created by Cellebrite. In 2024, Riyadh police succeeded in solving fraud cases 40% quicker based on the use of AI-based financial analysis to get investigators dedicating their time to strategic work as opposed to the monotonous task of processing data (Mohammed & Al-Abdul Rahman, 2024). As an example, AI systems processed terabytes of financial data in real-time and were able to detect suspicious transactions which otherwise could not have been detected manually. Such effectiveness is in line with the goal of Vision 2030 which aims at having a responsive justice system to facilitate case management and promote public safety. Nonetheless, the common usage depends on broader training in order to make the investigators capable of using the AI instruments, with the current structures training a small proportion of law enforcement officers (Veale et al., 2020). There is a necessity to invest in capacity building to get optimal value out of AI in the various regions in Saudi Arabia.

3.2 Improved Accuracy and Error Reduction

The use of AI improves the correctness of criminal investigations, reducing the element of human error that is so valid in Saudi Arabia with its Sharia-approved system of justice and where the focus on evidence must be precise. Manual identification of fingerprints yields 15 % less accuracy than those assisted by artificial intelligence in forensic laboratories, thus making the suspect identification more reliable (NIST, 2023). AI was used in 80 % of burglary cases in Jeddah, and the fingerprints successfully matched due to reduced human error in the cases of tiredness or improper supervision (Alshahrani et al., 2021). Such data-driven algorithms allow achieving stable results, which plays one of the key roles in creating just judicial processes according to the Islamic legal framework. An instance is that the AI inability to cross-refer bio metric information with national databases guarantees accuracy in identification of a suspect to minimize false positives. Nonetheless, an AI model must be routinely calibrated in order to ensure forensic soundness by correcting possible deviations in performance especially in culturally-graded settings (Crawford & Schultz, 2021). This further guarantees that AI continues to be a credible instrument in driving justice that acculturates to legal and ethical principles of Saudi Arabia.

3.3 Deeper Analysis of Complex Data

The ability of AI to analyze unstructured data, social media posts in Arabic and CCTV recordings help in shedding lighter on complex cybercrimes to aid proactive policing. SAR 1.5 billion in money operations were found out in 2024 due to the Natural Language Processing (NLP) models that identified 90 % of suspicious patterns in the social media and financial data (FATF, 2024). The cities of Riyadh and Dammam offered real-time analysis, which lowered the crime rates by 10%, as the police managed to understand where crime should happen and stop it (Alshahrani et al., 2021). As another example, AI was able to recognize and detect illicit financial flows using their trends in the unstructured data which could not be performed by humans. Someone should ethically monitor whether Personal Data Protection Law (PDPL) is followed, to protect the privacy of citizens with all the useful capabilities of AI (Crawford & Schultz, 2021). It is a necessary balance in preserving the faith of the population in the AI-powered policing system in the Saudi cultural context.

3.4 Judicial Support

Artificial intelligence used to generate evidence helps improve the performance of the judicial system because it presents interactive, reliable, and clear evidence in court. In 2024, 3D crime scene models powered by AI would enhance conviction rates due to murders by a 20 % margin as judges and prosecutors would view models as detailed, interactive visualizations (Smith, 2024). The stated financial data collected by AI was used in fraud trials in 70 % of the cases resulting in increased judicial confidence in the quality of evidence (Mohammed & Al-Abdul Rahman, 2024). These are instruments that make clarity in difficult cases where Sharia compliant norms focus on credible evidence. The lack of transparency in the evidence admissibility of AI contributed to the 2024 cases of cybercrime experiencing delays in 30 % because the legal frameworks regulating the use of AI evidence needed specific standards (Latham & Watkins LLP, 2024). Having these standards will help AI assist in equitable and effective judicial proceedings that further affirm the Saudi Arabian intentions to have a modern and fair justice system.

4. Challenges and Risks

Despite its benefits, AI's integration into Saudi criminal investigations faces multifaceted challenges.

4.1 Legal Challenges

It took 30% of cybercrime cases between 2024 and 2023 to reach adjudication due to the lack of explicit standards on the admissibility of evidence produced by an artificial intelligence (Latham & Watkins LLP, 2024). The PDPL of 2021 and the Anti-Cybercrime Law of 2007 lack specific protocols to be followed in using AI evidence and thus act as a legal framework with probability and uncertainty in the court process (Mutunga, 2021). As an example, downright rules regarding the admissibility of AI analyzed financial data were a barrier to the prosecution of fraud. There is a need to undertake a legal overhaul to outline specific procedures that would help ensure that AI-driven evidence does not isolate its precedent in shaping Sharia-compliant justice and the investigation process.

4.2 Moral Dilemmas

Facial recognition employed in 60 % of Riyadh cases is a type of AI surveillance that is a serious privacy concern outside the legal framework of PDPL (AL samara& Ghazi, 2024). Algorithmic biases are a threat to unjust profiling, and 10 % of the failures of the facial recognition will be in

2024 due to insufficient Arabic data, which will result in misidentifications (Bioamine& Gebru, 2020). Frequent audits and culturally informed algorithms are essential to reduce bias and guarantee equity and maintain faith in the criminal justice system in which AI may play a role.

4.3 Technical Problems

A security incidence that was carried out on one of the Saudi police databases in the year 2024 revealed weaknesses in the AI system by opening 10,000 records (BBC, 2024). It should also have strong cybersecurity safety bargains, including encryption and blockchain implementation, that will help secure sensitive data and in trust in AI-based inquiries.

4.4 Human Problems

The lack of training hinders the use of AI effectively as in 2024, 2,000 officers will be trained in its use (Alshahrani et al., 2021). To make the use of AI ethical, there is a necessity to expand education programs to provide investigators with competencies in using AI in accordance with the norms of the judicial and cultural framework of Saudi Arabia.

5. Regulatory and Ethical Framework

The legal structure that reflects the security of Saudi Arabia relies on PDPL and the Anti-Cybercrime Law but both of them should be updated in relation to AI-specific challenges. International standards, e.g., the EU AI Act (2021), focus on the transparency and risk criteria and provide an exemplar that customizes the Saudi implementation (European Commission, 2021). The AI Ethics recommendations of UNESCO, and the recent AI guidelines of Interpol provide further opportunities to incorporate standardized practice of evidence collection that increases the cross-border cooperation by 25% (Europol, 2024).

Such proposed solutions are:

- ✓ National AI Oversight Authority: Create within Nazaha to oversee AI systems similarly to how they now regulate dangerous-goods controllers, done throughout 2024, and minimize misuse within 40 per cent of what it would have done in fraud detection (Alaniz, 2025).
- ✓ Explainable AI and Bias Audits: Require clarity in the use of AI applications such as face recognition and within 2024 testing, the ideology will be reduced by 15 % (Alaniz, 2025).
- ✓ Sharia-Compliant Codes: Implement AI codes to match Islamic laws in such a way that they don't contradict the format of fairness and don't also quit the cultural criteria (Mansoor et al., 2024).
- ✓ Training Programs: Extend programs to assist in the training of investigators and judges, and in programs in 2024, it should reach an additional 25 % of the AI tool use (Alshahrani et al., 2021).

6. Future Vision

The future of AI in Saudi criminal investigation is the use of AI with new emerging technologies such as the blockchain and Internet of Things (IoT). Blockchain also provides water-tight records of evidence, which decreases the rate of disputes in 2024 trials of Nazaha by 20 % (Alaniz, 2025). The crimes have been detected in Riyadh using IoT-powered smart cameras with 85 % accuracy, reducing response times in Jeddah by 25 % (Mohammed & Al-Abdul Rahman, 2024). The smart city infrastructure of NEOM will decrease the response time by 30 % with the online content and social media analytics by 2026 (Europol, 2024). In 2024, 10,000 citizens got

educated through public awareness to trust in the use of AI in the process of justice (Mohammed & Al-Abdul Rahman, 2024). The need to address privacy violations should be ruled out through ethical governance and conformity with the Sharia to install trust in the masses (Selbst et al., 2021).

7. Case Study Insights: International and Local Successes

The FBI boasts the Next Generation Identification framework that can be used to achieve 90 % accuracy in biometric matching that processes 10 million records in 2023 internationally (FBI, 2023). The predictive policing decreased crime by 8 % in London, proving to save the UK 20 million in 2024 (Home Office, 2024). At the local level, the AI of Nazaha-based contract analysis detected SAR 500 million of fraud, and the biometric system of Absher identified 1,200 suspects in 2024 (AL samara& Ghazi, 2024). The precedent of ethical AI that caters to the Saudi needs was built by the automated processing and confidentiality-enabling features in the application of cyber harassment (Moala et al., 2018).

8. Recommendations for Future Research

8.1 Bias Mitigation in Arabic Datasets

In Saudi Arabia, face recognition technology, applied in 60 % of frictionless human face identification incidents in Riyadh in 2024, had a 10 % failure rate due to the insufficient Arabic collections, and thus having mistaken faces (Bioamine& Gebru, 2020). The studies need to focus more on creating rich repositories operating in line with the demographic and cultural environments of Saudi Arabia in terms of different skin tones and features, as well as traditional clothing patterns such as hijabs or thobes. Biases may also be mitigated by optimizing and training algorithms on data specific to the Arabic, relying on the methods of creating synthetic data (e.g., Antiflame) in order to reach demographically representative ratios. Cooperation with local universities and foreign professionals may make their algorithms take into consideration cultural peculiarities, which will improve justice and correctness in suspect identification and correlate with the principles of justice following Sharia.

8.2 Cybercrime Detection

The 20% rise in cybercrimes in 2024, including phishing attacks, underscores the need for AI-driven real-time detection systems (Europol, 2024). The studies should be directed towards creating sophisticated Natural Language Processing (NLP) and anomaly detection models to detect phishing attacks within communications carried out in Arabic which is the language of dominance in Saudi digital space. The inquiry into involving AI with blockchain in securely logging data can help increase traceability when dealing with cybercrime. These could be piloted in Riyadh and Jeddah, which is directed in accordance with the Anti-Cybercrime Law (2007), and safeguarding sensitive data as stated in the Personal Data Protection Law (PDPL), by developing Saudi Arabia cybersecurity system.

8.3 Public Trust

In 2024, 40 % of Saudi citizens reported being concerned about their privacy when it comes to AI-based justice, especially facial recognition and surveillance system (Latham & Watkins LLP, 2024). The subject matter should be tested to determine the perception of citizens by carrying out national studies; with emphasis on the cultural attitude towards the use of AI in law enforcement and the law. Addressing the misconceptions and earning the trust will be possible by involving communities through public forums and educational campaigns, which was the case observed in

2024 when 10,000 citizens were reached (Mohammed & Al-Abdul Rahman, 2024). Experiments ought to also determine the efficiency of the naked AI systems, like explainable algorithms, to eliminate the issues of privacy whilst proposing the Sharia compliant mediation to win the trust of the community in the justice given in the AI-based justice system.

9. Implementations

Artificial intelligence (AI) Adoption in Saudi Arabia criminal justice system has also been strategic to ensure the adoption aligns to the objective of Vision 2030 in modernizing the security systems within the country and yet meeting the Sharia compliant standards. Notable applications reveal how AI is transforming other areas of investigations to be more effective, precise and reduce bias in the judicial system.

9.1 Practical Implementations

By 2024, artificial intelligence-based tools such as the Cellebrite Universal Forensic Extraction Device (UFED) were expected to be placed in cybercrime departments and could process digital evidence of smartphones and computers at an 85 % rate of recovery in a process that is half as long as before (Horsman, 2020). SFIU applied machine learning and identified 95 % of suspicious transactions that revealed illicit flows of SAR 1.5 billion (FATF, 2024). Facial recognition AI of the Absher platform decreased 70 % of residency and visa fraud with 60 % of suspects detected on 1200 cases (AL samara& Ghazi, 2024). In Riyadh, 3D crime scene modeling powered by AI led to the enhancement of the clarity of evidence by 25 % in cases of homicide, which assisted in court procedures (Smith, 2024). Natural Language Processing (NLP) was adopted at the Saudi Anti-Corruption Authority (Nazaha) to examine case files that identified a SAR 500 million falsification in contracts (Alaniz, 2025). Of interest is the example of the AI-based cyber harassment reporting app by Fahad Abdullah Moala, which involves N-gram, sentiment analysis to maintain victim confidentiality and electronically process the cases to deal with crimes such as bullying and defamation (Moala et al., 2018). It currently has a pilot stage that is working in 2024 in which cyber abuse is minimized by 95% and adheres to Saudi culture and PDPL.

9.2 Strategic Initiatives

Saudi Arabia has undertaken strategic initiatives to help adopt AI. In 2024, 10,000 citizens were educated through campaigns promoted by the government to promote confidence in AI-delivered justice (Mohammed & Al-Abdul Rahman, 2024). Explainable AI and bias audit under pilot programs of Nazaha reduced misuse in fraud detection by 40 % (Alaniz, 2025). In 2024, 2,000 officers under trainings were shown to be able to use AI tools but greater scope is required (Alshahrani et al., 2021). By integrating with emerging technologies such as blockchain and IoT and trialed in Riyadh and Jeddah, the integrity of evidence was enhanced and the response time shortened by 25 % (Europol, 2024). The upcoming use of IoT and social media analytics in NEOM smart-city infrastructure will further add to the beneficial effects and result in a 30 % decrease of response rates by 2026.

10. Conclusions

AI has improved Saudi Arabian criminal investigation significantly which fits into the vision 2030 in terms of efficiency, accuracy and judicial results. Application of tools (UFED, biometric systems, NLP) have simplified the investigation process, including outstanding achievements by 2024 of verification of frauds (2 billion saved) and detecting suspects (60 % official case

resolution rate). The cyber bullying app is an example of ethical innovation that safeguards the victims and does not discount the Sharia or PDPL requirements. Nevertheless, there are vexations, like legal uncertainties that hold up 30 % of cases of cybercrimes, privacy issues on AI surveillance, or 10 % fail rates face recognition attributable to the small size of the Arabic datasets (Bioamine& Gebru, 2020). The technical issues like the data breach in the year 2024 that leaked 10,000 records and a lack of officers training highlight that strong solutions are required (BBC, 2024). Ethical use of AI will be achieved due to a proposed national AI regulator under Nazaha per international standards (such as the EU AI Act), increased training and Sharia-compliant procedures. The role of AI will further be reinforced in the future that involves research on bias mitigation strategies, real-time identification of cybercrimes, and its trustworthiness among people. With these issues in mind, Saudi Arabia is capable of maintaining a more intelligent but more equitable system of justice that will balance the technical development and considerations of culture and ethical requirements, generating support among the population and creating the integrity of justice.

Funding

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (GRANT KFU254089)

References

AL samara, M., & Ghazi, A. (2024). AI in Saudi criminal justice: Opportunities and challenges. *Journal of Middle Eastern Law*, 12(3), 101–120. https://www.researchgate.net/publication/384910406_The_Role_of_Artificial_Intelligence_in_Criminal_Justice

Alshahrani, R., Dennehy, D., & Mäntymäki, M. (2021). AI in Saudi judicial systems: Legal and ethical considerations. *Computer Law & Security Review*, 41, 105–115. https://www.researchgate.net/publication/387268650_Justice_in_the_Age_of_Artificial_Intelligence_A_Comparative_Study_of_the_Legal_Framework_for_Forensic_Evidence_in_Saudi_Arabia_and_Global_Practices

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2020). Machine bias: Investigating the algorithms that control our lives. *ProPublica*. https://www.scirp.org/reference/referencespapers?referenceid=3337609

BBC. (2024). Saudi police database breach exposes 10,000 records. *BBC News*. https://www.bbc.com/news/articles/cj4ek9njknvo

Berk, R. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. *Annual Review of Criminology*, 4, 209–237. https://www.annualreviews.org/doi/10.1146/annurev-criminol-051520-012342

Buolamwini, J., & Gebru, T. (2020). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Casey, E. (2021). Advances in digital forensics: Emerging trends and challenges. *Digital Investigation*, 36, 100–110. https://www.researchgate.net/publication/389631795_Emerging_Trends_in_Digital_Forensics_Investigating_Cybercrime

Crawford, K., & Schultz, J. (2021). AI systems as state actors: Privacy and surveillance

implications. *Columbia Law Review*, 121(5), 1235–1280. https://columbialawreview.org/wp-content/uploads/2019/11/Crawford-Schultz-AI_systems_as_state_actors.pdf
European Commission. (2021). Proposal for a regulation on artificial intelligence (AI Act). *EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206#:~:text=The%20proposal%20sets%20harmonised%20rules,future%2Dproof%20definition%20of%20AI.
Europol. (2024). AI-driven counter-terrorism: Social media monitoring. *Europol Annual Report*. https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf
FATF. (2024). AI in anti-money laundering: Global trends and challenges. *Financial Action Task Force Report*. https://www.fatf-gafi.org/en/home.html
FBI. (2023). Next Generation Identification: Annual performance report. *Federal Bureau of Investigation*. https://www.fbi.gov/file-repository/pias/pia-next-generation-identification-biometric-interoperability.pdf
Home Office. (2024). Predictive policing: Impact assessment 2023–2024. *UK Government*. https://post.parliament.uk/use-of-digital-scientific-and-other-technologies-by-the-police-and-wider-criminal-justice-system/
Horsman, G. (2020). Digital forensics: Challenges in the cloud. *Forensic Science International*, 32, 200–210. https://commons.erau.edu/jdfsl/vol15/iss1/3/
Hovy, D., & Prabhumoye, S. (2021). NLP in law enforcement: Opportunities and challenges. *Computational Linguistics*, 47(3), 567–598. https://pubmed.ncbi.nlm.nih.gov/35864931/
Howell, B. (2024). Regulating artificial intelligence in a world of uncertainty. *American Enterprise Institute*. https://www.aei.org/research-products/report/regulating-artificial-intelligence-in-a-world-of-uncertainty/
Johnson, M. (2024). Generative AI in criminal investigations: Case file summarization. *Journal of Policing Technology*, 12(1), 45–60. https://www.sciencedirect.com/science/article/pii/S0264275124006863
Latham & Watkins LLP. (2024). In-depth: Artificial intelligence law in Saudi Arabia. *Legal Review*. https://www.lw.com/admin/upload/SiteAttachments/Lexology-In-Depth-Artificial-Intelligence-Law-Saudi-Arabia.pdf
Mansoor, M., Paul, J., Saeed, A., & Cheah, J. H. (2024). AI in criminal investigations: Ethical implications. *Journal of Business Research*, 176, 114591. https://www.researchgate.net/publication/381955225_Ethical_Considerations_in_Use_of_Artificial_Intelligence_in_Digital_Marketing
Mohammed, A. F. A., & Al-Abdul Rahman, H. (2024). The role of artificial intelligence in fraud detection in Saudi Arabia. *Journal of Arts, Literature, Humanities and Social Sciences*, 100, 472–506. https://www.researchgate.net/publication/377983587_The_Role_of_Artificial_Intelligence_AI_on_the_Fraud_Detection_in_the_Private_Sector_in_Saudi_Arabia_Introduction
Mutung'u, G. (2021). Data protection in Saudi Arabia: Legal frameworks. *African Journal of ICT Law*, 15(2), 89–104. https://migrationletters.com/index.php/ml/article/view/7684
Ng, J. (2024). AI-driven policing: Real-time facial recognition. *Asian Journal of Criminology*, 19(1), 33–50. https://www.lco-cdo.org/wp-content/uploads/2025/04/LCO-AI-in-Criminal-Justice-Paper-2-Law-Enforcement-Use.pdf
NIST. (2023). Facial recognition technology evaluation: Accuracy benchmarks. *National Institute of Standards and Technology*. https://pages.nist.gov/frvt/html/frvt11.html
Raso, F., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2020). Artificial intelligence &

human rights: Opportunities & risks. *Berkman Klein Center*. https://dash.harvard.edu/entities/publication/30cbf82e-bf6f-419f-a634-0d5acd6f647e

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2021). Fairness and abstraction in sociotechnical systems. *ACM Transactions on Computer-Human Interaction*, 28(4), 1–29. https://www.researchgate.net/publication/330264946_Fairness_and_Abstraction_in_Sociotechnical_Systems

Smuha, N. A. (2020). The EU approach to ethics guidelines for trustworthy AI. *Computer Law & Security Review*, 39, 105–120. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3443537

Wang, Y., Zhang, L., & Chen, X. (2021). Virtual reality in forensic investigations: A review. *Journal of Forensic Sciences*, 66(5), 1723–1735. https://www.researchgate.net/publication/357265368_Forensic_Science_Education_by_Crime_Scene_Investigation_in_Virtual_Reality

Yahaya, N., Kamin, Y. B., & Alamri, M. (2018). Integrated-system to minimizing cyber harassment in kingdom of Saudi Arabia (KSA). *International Journal of Engineering & Technology*, *7*(4), 2192-2196. https://core.ac.uk/download/pdf/334606563.pdf