

Justice in the Age of Artificial Intelligence: A Comparative Study of the Legal Framework for Forensic Evidence in Saudi Arabia and Global Practices

Dalia Kadry Ahmed Abdel Aziz¹

Abstract

This research paper seeks to explore a potential legal predicament, that arises from integrating artificial intelligence (AI) in extracting and analysing forensic evidence in the Saudi Arabian judicial system. Now, with the rapid growth of AI technologies and its application in criminal investigation, becoming more common, there are many legal and ethical questions that arise. The paper also addresses some important issues, such as the reliability of evidence generated by AI, its admissibility in the courts, and the protection of the defendants' rights to privacy. The paper then delves into a study of the available legal frameworks in the Kingdom of Saudi Arabia alongside a comparative study of some international systems: the United States, the United Kingdom, the European Union, and the legal framework of China. It shows important lessons learned from these jurisdictions. Furthermore, the findings also suggest several legal and procedural reforms that could be implemented to improve the efficiency and fairness of the Saudi judicial system. These include, inter alia, possible standardization in terms of admissibility of technical evidence, increased transparency in the algorithms used, and judges that have legal and technical training. Thus, the study seeks to suggest pragmatic recommendations to strike the balance between the required efficiency propelled by AI technologies and the governing principles of justice in the Saudi legal environment, which based on Islamic law.

Keywords: *Artificial Intelligence, Forensic Evidence, Saudi Judicial System, Islamic Sharia, Algorithmic Bias, Admissibility of Evidence, Privacy Protection, The defendant's right to privacy.*

Research Methodology

The study is descriptive and analytic, as it begins with the detection of the problems of integrating (AI) technologies in the judicial system of Saudi Arabia, as well as the anticipated legal and ethical issues which may appear because of integrating (AI) technologies. It reviews previous literature data on forensic evidence, which serves as the foundation to understand the current state of the art of AI to ensure that research and application are used effectively through AI. The methodology further includes comparing the Saudi judicial system to other legal systems in the United States, the UK, Ecuador, and China, to learn evaluations of other countries in this regard. This study draws on an analysis of existing data, laws, and regulations on the use of artificial intelligence and examines its compatibility with Islamic standards and principles of justice. At the end of this study, we offer guidelines on how to develop a holistic system to manage AI in forensic evidence, according to the results which emerge after analyzing and comparing legal frameworks that require a solution concerning the proportioning of artificial intelligence development and human protection of basic rights.

Introduction

Thanks to the rapid advancement of artificial intelligence (AI) technologies, this innovation is on the brink of becoming fundamental in various critical sectors, particularly within the judicial system. AI applications, such as facial recognition, voice analysis, and image processing, greatly enhance criminal investigation processes and enable the digital collection and examination of evidence. However, these considerable benefits come with significant legal and ethical concerns, raising questions about the reliability of forensic evidence, the risk of algorithmic biases in such evidence, and the defendant's right to privacy.

In the context of the Saudi Arabian judicial system, which primarily relies on Islamic Sharia as its legislative foundation, the integration of AI in evidence gathering presents numerous legal hurdles. Islamic Sharia places a strong emphasis on justice, the rights of defendants, and the safeguarding of privacy, necessitating

¹ Assistant Professor of Criminal Law, Prince Sultan University -Riyadh, Kingdom of Saudi Arabia; Dkadry@psu.edu.sa.

specific regulations, to ensure that the adoption of modern technologies does not contravene Sharia principles. Islam delineates a clear distinction between permissible and impermissible evidence in court, and the substantial use of AI tools must be meticulously aligned with Sharia-based evidentiary standards, given the inherent principles that mandate a minimum level of integrity and transparency in investigations before evidence can be acknowledged.

This research aims to explore the legal frameworks surrounding the prospective application of AI in Saudi Arabia's criminal investigation sector, along with the legal and ethical challenges that may arise. It will also consider the judicial systems of other nations that have made progress in implementing such technologies. Furthermore, the study will analyze legal frameworks pertinent to the utilization of AI in evidence, highlighting the necessity for legislation to be modified to comply with Islamic Sharia law, thus enabling the use of these technologies without infringing on humans' rights or the principles of justice.

The State of Artificial Intelligence Usage for Forensic Evidence in Saudi Arabia

The deployment of AI technologies in the collection and analysis of forensic evidence, has become increasingly relevant across legal systems, globally as the field of artificial intelligence (AI) develops rapidly. Saudi Arabia has incorporated AI technologies into its criminal investigation offices, including facial recognition technologies, voice recognition, and image processing. Although the prospects of these technologies are promising for adding value to the judicial system, the latter encounters major hurdles concerning the abduction of AI evidence assistances.

One of the biggest issues is the lack of clear laws governing this kind of evidence. Furthermore, the tension between harnessing technological efficiency and fulfilling the requirements of justice is still very much alive. To remedy these shortcomings, the law must develop in a way that adequately strikes a compromise between innovation and individual protection.

The Role of AI in Modern Criminal Investigations

Saudi Arabia, in recent years, has significantly embraced the world of artificial intelligence (AI) technologies for assisting in criminal investigations. Perhaps the most significant of these is the use of facial recognition technology, which has come to play an essential role in identifying and tracking suspects in public locations and airports. This technology allows law enforcement agencies to match images with existing databases to identify individuals (Al-Faiz & Al-Juhani, 2020).

Moreover, voice recognition systems have also been used in criminal investigations to analyze phone calls and glean useful information from chatting to fill in investigation clues (W. J. H. & Z. T. R., 2019). Image forensics is another important application: The analyst can investigate changes made in crime scene photos, X-ray, medical imaging, and much more. For example, they can be used to analyze crime scene photographs or X-ray data to uncover markers potentially connected to criminal behavior (W. J. H. & Z. T. R., 2019).

Such progress does hold revolutionary potential for expanding law enforcement's ability to detect evidence that may not be discovered through other, traditional means. But with all the advantages these technologies provide, there are also significant challenges to their use within the Saudi judicial system. The lack of regulations about what constitutes admissible evidence and where AI-generated evidence fits within that structure poses one of the most pressing challenges (Mansoor et al., 2024). Moreover, the trade-off between technical efficiency and the requirements of criminal justice is still a fundamental concern. It is crucial to strike a fine line between utilization of these contemporary means and protection of individual rights and the validity of legal processes (Al-Saadi & Al-Hamzi, 2022).

The Legal and Procedural Challenges in Admitting AI-Generated Evidence in Saudi Courts

As exciting as this may sound, there are many legal barriers that the Saudi judicial system faces, when it comes to the increasing use of artificial intelligence in criminal investigations. To begin with, there is no specific legislation that governs how evidence generated by AIs will be treated as admissible in courts. This

necessity calls for the establishment of distinct legal standards specifying the conditions under which such evidence must be assessed and under which it is acceptable to use it (Alshahrani et al., 2021)

Secondly, there is a major tension between technical efficiency and the demands of criminal justice. These accurate results can actually be manipulated and biased depending on the algorithms programmed. Such issues lead to questions about the reliability of evidence produced by these technologies more generally, particularly in high-stakes cases that have important consequences for the rights of defendants (Alshahrani et al., 2021).

Recent legal and regulatory endeavours (e.g., the issuance of ethical principles for AI by the Saudi Data and Artificial Intelligence Authority (SDAIA) ,2023) point toward the need for an integrated legal framework. A framework of this kind is needed to ensure that this technology is used in criminal investigations, in a way that is both transparent and secure, while also protecting individual rights and promoting justice (Latham & Watkins LLP, 2024; Alsamara, & Ghazi ,2024).

The Concerns of AI-Generated Evidence in a Legal and Procedural Context in Saudi Courts

The Saudi judicial system faces a number of legal hurdles, despite the growing use of artificial intelligence in criminal investigations. Initially, there is no clear legislative framework around the acceptability of evidence generated by AI technologies in courts. Thus, there is an urgent need to develop precise legal standards that stipulate how such evidence ought to be assessed and under what circumstances it is admissible (Alshahrani, Dennehy, & Mäntymäki, 2021).

Second, much of the problem is the tension between technical efficiency and the needs of criminal justice. Although AI technologies achieve near accuracy in their results, these technologies can still be biased, as algorithms can be programmed or want naturally. This presents doubt as to the reliability of evidence extracted from these technologies, especially in cases of considerable consequences for the rights of defendants (Alshahrani, Dennehy, & Mäntymäki, 2021).

Recent legal and regulatory actions illustrate the emphasis on a unified legal framework, the issuance of ethical principles for AI by the Saudi Data and Artificial Intelligence Authority (SDAIA) in 2023, being one of the most relevant steps to highlight here in this regard. This framework is necessary to create transparency about the use of this technology in criminal proceedings and to respect individual rights and constitutional guarantees in each case

Reliability and Accuracy Issues

With the absence of clear legal standards to regulate such evidence before the courts, it can be an obstacle in the Saudi judicial system, regarding the admissibility of AI evidence. Because there is a device for the application of AI in selective crime cases (including facial recognition and voice analysis), It is essential to engage with these efforts due to the increasing stock of AI technologies, which used in criminal cases. These problems have raised concerns about the contestability of AI-generated evidence, especially in absence of legally binding standards and rules, regarding the nature of evidence, particularly given the potential corruption of the evidence based on technical errors and biases in AI products that can potentially undermine correctness.

For instance, while facial recognition technology is more sophisticated today through training with extensive datasets, studies conducted by the U.S. Federal Bureau of Investigation (FBI), identified a problem of racial bias among algorithms used in criminal investigations, causing some of the results to be imprecise, especially for people of darker skin (Garvie, Bedoya, & Frankle, 2016). Mistakes like those could raise questions about the admissibility of AI-based evidence in court.

In this case, the evidence presented during the trial of facial recognition was challenged in the U.K. An independent report commissioned by police in London concluded, that the system was too flawed to be used reliably in a legal context. This made the court somewhat dubious regarding the credentials of this

type of evidence, and the employment of it in the courts (Fussey & Murray, 2019). Such instances call into action the creation of strict legal standards to appraise and assess the reliability of a simulated test of reliability of AI-generated evidence in accordance with legal code in Saudi.

In part, that's led to local efforts that are developing legislation around AI-based evidence. For instance, the Saudi Shura Council published a report (Saudi Shura Council, 2021), which recommended updating the legislation in order to cover the AI technologies, and to ensure that evidence obtained via the implementation of those technologies will be subjected to legal scrutiny. Likewise, in 2022, the Saudi Ministry of Justice launched the E-Litigation System Project to improve the use of digital evidence in court proceedings (Saudi Ministry of Justice, 2022). These projects reflect the Kingdom's keen interest in further developing its legislative system to keep pace with contemporary technologies while maintaining its alignment with the imperatives of criminal justice.

The Federal Rules of Evidence of the US are one of the key international guiding norms to provide the operational framework for assessing the accuracy and reliability of digital evidence that is resulting from AI technology. To this aim, such guidelines define detailed criteria for the submission of digital evidence in the court.

Specifically, the Federal Rules of Evidence have certain practices that account for the assessment of modern technology-based evidence, such as AI-based evidence. For example, Rule 901 applies to "authentication" and "reliability" of digital evidence, which is evidence material that has been generated from advanced technological systems. This document, Rule 702, articulates the standard for the admissibility of the qualifications of the expert who testifies to this evidence before it can go to trial (Hoffman et al., 1992).

Moreover, the establishment of an open certification authority, in partnership with the National Institute of Standards and Technology (NIST), will be critical to developing standards and protocols to evaluate digital evidence and AI systems within legal frameworks. This ensures the credibility and reliability of evidence in the courts.

AI Technology in the Context of Digital Evidence: A Comparative Study of Current Saudi Standards Versus Other International Judicial Systems

The application of artificial intelligence technologies results in evidence whose legal validity is still being grappled with, regarding the clear standards and mechanisms for its regulation and assessment in the courts, in light of the absence of serious implementation or acceptability by the Saudi judicial system. Although AI is being used more frequently in criminal investigations today — for example, with facial recognition and voice analysis technologies — there is an urgent need for a legal framework to be developed better to ensure accuracy and reliability of this kind of evidence. This is especially significant as there are no clear laws governing any digital evidence relating to AI technologies, leaving courts open to these challenges regarding their validity due to technical errors or biases within data.

With rules of relevance, admissibility, and probative force, the legal systems of Australia, the United States, and the United Kingdom thus represent much more overt and formal standards of regulation and evaluation of digital evidence. The Federal Rules of Evidence are a foundational guideline in the United States for handling how digital evidence is admissible in courts. Rule 901 is clear on the need to establish the "identity" and "reliability" of digital evidence, and Rule 702 outlines the qualifications of experts who use such information, ensuring it has been compiled using accurate and credible methodologies. The National Institute of Standards and Technology (NIST) also offers a regulatory framework for the evaluation of digital evidence and AI-based systems, thus increasing their credibility in U.S. courts (National Institute of Standards and Technology, 2021).

In the UK, the London Metropolitan Police and other judicial institutions, have independently assessed the use of facial recognition technologies. These assessments found the systems were not accurate enough to be reliable legal tools. The skepticism surrounding the reliability of digital evidence has led the British courts

to seek stringent legal standards when it comes to the use of AI in a judicial proceeding (Fussey & Murray, 2019).

Evidence laws in Australia set clear standards for the admissibility of digital evidence in the judicial system. The acceptance of digital evidence is governed by acts like the Evidence Act 1995, which require proving the authenticity of the evidence, to check if the digital evidence has been altered or manipulated with the help of advanced techniques. These provisions are similar to those applicable in the U.S. when assessing the reliability of evidence. Under its judiciary principles, Australia mandates the effective handling of digital evidence only by accredited practitioners to maintain reliability standards (see Australian Law Reform Commission, 2015).

On the other hand, the Saudi legal system cannot be considered comprehensive and adequate, even with future initiatives such as the Electronic Litigation System Project initiated by the Saudi Ministry of Justice. Therefore, a general framework for the assessment of evidence resulting from the application of artificial intelligence techniques remains absent. This constitutes a vital step to develop the Saudi system to correspond to modern international legal practices, such as the United States Federal Rules of Evidence, in addition to the systems in place in the United Kingdom and Australia (Howell, 2024).

Examining these practices will not only provide insight into the various approach's countries adopt toward AI-derived evidence but also highlight the need for Saudi Arabia to ensure the fairness and reliability of any data used in their criminal proceedings. The development of these standards is important to address technical and ethical issues and to reflect global best practices.

The Authority strives to ensure that the ethics of protecting rights are met

One of the challenges when applying artificial intelligence technologies to judicial systems is the protection of individuals' rights. In Saudi Arabia, privacy is a basic right, and its violation without legal justification is a violation of Islamic principles. The Quran says: "And do not spy on one another, nor speak ill of one another behind their backs" (Al-Hujurat: 12).

Saudi Arabia is working to protect people's rights in its new use of artificial intelligence, such as the systems used for facial recognition and data analysis, through privacy legislation. Regarding laws governing personal data management, the "Personal Data Protection Law," released in 2018, requires the protection of each person's personal information and label, and clearly specifies the limits to data collection and use. The system is based on Islamic legislation, but it is also consistent with international agreements, especially regarding individual rights. (Albakjaji, & Almarzouqi, 2024).

When any such matter came to the attention of one of the Muslim governor in the early period of Islam, one would inquire, one would investigate, one would ascertain the facts, and one would gather information that would ensure the actual deliverance of justice; such was the approach of Omar ibn Al-Khattab, may God be pleased with him, during his era as he implemented the principles and the spirit of Islamic law throughout his rule, until one man, he heard, had drunk alcohol in his home. He sent people to spy on him. When Umar ibn al-Khattab used to catch someone doing a crime, he would want to punish, but when he learnt that this proof was collected through spying and was not legitimate, he would say, he declared that the evidence has no value and cannot be used against the person. "O Allah! I presented nothing to you except for a legitimate proof," thereby affirming the privacy as being sacred and evidence obtained with a breach of that privacy is not acceptable before the shariah courts either.

Such an incident is among the well-known ones that happened in Islamic Civilization, where Sharia law disallowed the use of evidence caught in an illegal way, for instance, spying on people in their private life, hence, ensured a structure applicable for safeguarding privacy (Afsaruddin, 2020) This is mirrored by modern legislation. An example of this includes the 1974 Federal Privacy Act in the United States, which requires the protection of citizens' personal data and limits data collection and use in technology applications (Howell, 2024). In the United Kingdom, the UK Data Protection Act 2018 requires organizations to obtain individuals' consent before processing their personal data, and it places controls on

the use of sensitive personal data, including biometric and behavioral information. This operates up to a few bytes of information.

These legislations correlate with Islamic history, suggesting that privacy protection is an essential principle to achieve in every judicial system across the world, including Saudi Arabia or the international systems, to ensure the respect of the human rights of individuals and to shield them from any abuses that can stem from the use of AI technologies

International Law and Policy on AI Usage in Judicial Processes

As the newest generation of artificial intelligence technologies, threatens to rapidly proliferate across international legal systems, the speed with which these technologies are absorbed into judicial systems, which raises questions in novel ways about their potential prevention, use in investigations and trials alike (Binns, 2018). This chapter provides insight from international legal systems such as the American, European, and Chinese systems, regarding the application of artificial intelligence within judicial procedures. It further discusses the requirements for the admissibility of scientific, technical evidence in such systems, the necessity for balancing privacy protection and the integrity of technology use. Knowing these legal experiences provides important lessons that may help with developing the Saudi judiciary system to address the challenges posed by artificial intelligence.

A Framework for the Evaluation of Scientific Evidence in the U.S. Courts

The American judicial system has a systematic view of the doctrine of scientific and technical evidence, which is presented to ensure the credibility and reliability of all scientific and technical evidence in the court. The Frye standard is based on the case *Frye v. United States* (1923), which determined that scientific evidence must be "generally accepted" in the relevant scientific community to be admitted (*Frye v. United States*, 1923). This standard has been adopted in a few states of the Union, where evidence is admitted only in accordance with strict scientific traditions, so that the risks of unreliable or untested techniques are curtailed.

As the U.S. judicial system has evolved, it introduced the Daubert standard from the Supreme Court case *Daubert v. Merrell Dow Pharmaceuticals* in 1993, to consider what constitutes admissibility of scientific evidence and opened the parameters under which scientific evidence is exposed and examined in the court of law. That standard allows the judge to evaluate evidence against several critical factors — testability of methodology, error rates, peer review, and general acceptance in the scientific community, among others. This enables judges to act as “gatekeepers” to determine that scientific evidence presented is scientifically valid prior to submission to the jury (*Daubert v. Merrell Dow Pharmaceuticals*, 1993).

The use of artificial intelligence technologies in U.S. criminal cases increasingly demands scrutiny of the evidence derived from them. To take just one example, in the case of *State v. Loomis*, the thing that had the court worried about algorithms included the push for algorithmic transparency in data analysis. Therefore, algorithms should be interpretable, for parties in dispute to conduct an audit of them and improve the trustworthiness of the evidence (*State v. Loomis*, 2016).

Many of the cases are also related to algorithm biases, that could lead to unfair results for some categories of people. Some examples include facial recognition programs that exhibited low accuracy rates when identifying individuals of certain racial backgrounds (Pathak, et al. 2021). Within this context, U.S. courts attempt to ensure that bias is not embedded in the tools that are being used to track crime. Thus the quality of decision-making regarding crime can be measured within this context.

In U.S. courts, cases surrounding artificial intelligence also place significant weight on ethics and safeguarding privacy. Courts are interested in verifying that the technology being utilized does not violate rights protected by privacy laws, such as the Fourth Amendment of the U.S. Constitution (“Fourth Amendment,” 2020), which safeguards against unreasonable search and seizure. Additionally, these

measures are consistent with the ethics principles set out by the Saudi judicial system, which places individual privacy protection among its responsibilities (Alsharif, 2021).

The reliance on the evidence of science and technology is an integral part of the judicial procedure in Saudi Arabia, in the investigation of crimes. That practice has evolved with the rest of criminality and the new scientific methods of pinpointing, collecting evidence to chase those crimes, including DNA testing, surveillance programs, and digital evidence. Based on studies done, this type of evidence has begun to be adopted in the Saudi system under the umbrella of Islamic law, if it does not contradict the concept of justice and the preservation of personal rights (Al-Dosary, 2019).

One of the most significant general foundations of modern science, is the utilization of contemporary scientific environmental evidence, such as chemical and technological analysis, which is presented in support of enhancing the potential, to verify the particulars surrounding the committed crimes, and in accordance with the interest demonstrated by the judicial system in Saudi Arabia, also developed in line with the responsiveness to the importance of going through such evidence following sublimated Islamic legislation that was founded since those early days of Islam. Although there is still much focus on how modern technologies in the criminal justice system can work together with the existing framework to improve efficiency for investigations and trials (Kang et al., 2023), this should be taken with caution as the judiciary system is primarily based on Islamic law.

The European Angle: The Impact of the General Data Protection Regulation (GDPR) on Artificial Intelligence Utilization in Criminal Cases

The new regime will have a major impact on how it will interact with the Artificial Intelligence (AI) adopted for criminal investigations in Europe, in the form of the General Data Protection Regulation (GDPR) adopted in 2018. It provides information on personal data protection and privacy rights, throughout the European territory and its affectation on the operative application of AI technologies in law enforcement and justice. Natural Language Processing (NLP), “virtual detectives,” and online gathering of evidence are a few examples of tools used in the investigation and prosecution of criminal cases, which are subject to this framework. It states that data processing, the use of which must also comply with privacy principles, including tools powered by artificial intelligence, may not violate the privacy rights of individuals. Specifically, AI systems that handle personally identifiable information must adhere to principles such as data minimization, purpose limitation, and transparency (Voigt & von dem Bussche, 2017).

While AI technologies may afford law enforcement powerful capabilities—leveraging, for example, predictive policing applications and facial recognition technologies—they remain regulated under the system established by the General Data Protection Regulation (GDPR) to ensure the rights of individuals to privacy. For example, part of the provisions of the relevant GDPR is that, if data processing is carried out without the necessary consent or involves a high risk of compromising individuals' freedoms and rights including sensitive data this includes race or ethnic origin (Kuner et al., 2020)

This is a balancing act because, on one hand, AI technologies can improve the efficiency of crime decisions, but their use must also be balanced by adequate measures to ensure the protection of people. While law enforcement agencies and courts use AI to help them solve crimes more efficiently, they must also make sure the technology doesn't overstep the mark in other areas, like surveillance or data exploitation. Apart from the moral duty for responsible AI use, the AI Design Process proposes that misapplication of AI (e.g., mass surveillance and predictive policing functionalities) can harm people (Binns, 2018). European lawmakers and the judiciary are hence invited to search for solutions, that will allow effective deployment of AI in the context of crime, while respecting fundamental rights, including privacy.

In particular, the European framework allows for regular discussion and updates in certain instances, in which using AI tools could violate individual privacy rights, as defined in the regulation. Most importantly, it indicates a straightforward appeal to rigorous rule of law, transparency, and accountability frameworks, that can ensure the ethical and legal use of AI technology in criminal inquiries, without undermining individual rights or the principles of justice (Zanfir, 2020). Furthermore, ongoing discussions regarding

potential tensions between the General Data Protection Regulation (GDPR), that is already in force and the upcoming Artificial Intelligence Act due in 2024 also outline important compliance questions regarding compatibility. These are the principal outputs from such a complex wave of regulation, with maybe the different regulations come together, somehow be complementary in terms of aims towards an ethical usage of AI within a legality scope that the same regulations seem to project, reels again possible challenges from these regulations around enforceability and implementational nuance, balance innovation with privacy stakes(Butt, 2024)

Chinese Approach: Artificial Intelligence Integration in Judicial System and Ensuring the Integrity of Forensic Evidence

One of the leading countries in applying artificial intelligence to the judiciary, China is also seeking ways to improve efficiency and take pressure off courts. Automation is applied to judicial procedures to expedite and ensure easy access through “smart courts.” A crucial purpose of these systems is to increase effectiveness and processing, as digital technologies accelerate case processing and decrease delays (Papagiannas & Junius, 2023). At the same time, the emphasis is on preserving the integrity of forensic evidence and transparency in developing these technologies, to uphold people's rights under an increasingly post-digital transformation (Wang & Tian, 2023).

While the above advances in China are impressive, the Chinese judicial system approaches AI in a way quite distinct from the American system. Given the focus on increasing efficiency and relieving pressure on the judicial system, China's smart courts are designed to improve the productivity that the Chinese system prioritizes. On the other hand, here in the US, the debate is centred around privacy and individual rights in the age of AI. In some cases, there are concerns about whether AI will help protect personal information or lead to discrimination (Wang, 2020). This indicates the American system being more protective of individual rights than the Chinese system, as the latter prioritizes efficiency in adjudicating cases (Wang & Tian, 2023).

In Saudi Arabia, AI technologies are slowly entering the judicial system in a bid to alleviate pressure on services, whilst increasing the efficiency and integrity of the judicial process under "courts of the future." For example, AI is implemented in analyzed forensic data under adequate legal measures aimed to apply justice. So, it would take the Saudi model, which is neither the Chinese nor the American, to see how deep the protection of rights is.

Legal and Procedural Reforms for the Saudi Judicial System: Exploring the Impact of Artificial Intelligence on Forensic Evidence

Considering the presenters' review of the legal status of the subject under study, it is now necessary to create the legal and procedural framework, that regulates the use of forensic evidence derived from said technologies. This chapter presents the reforms needed in the Saudi judicial system, since it should lawfully consider technical evidence while helping the transparency and integrity of algorithms. That also includes discussing the need for legal technical capacity building among judges and lawyers to leading the proper handling of such evidence. The final section discusses how technical and legal experts can work together to provide practical solutions that can support rapid technological innovation.

Creating a Legal Framework to Guarantee the Admissibility of Forensic Evidence and Algorithmic Transparency

AI In the Judicial System

The incorporation of artificial intelligence in the Saudi judicial system, requires a detailed legal framework to govern the usage of forensic evidence provided by these technologies. This framework is vital to guarantee, that the application of artificial intelligence in criminal investigations is accurate and clear. To do so, it's essential for the Saudi justice system to draft legislation, that clarifies the acceptable standards for technical evidence and the conditions to ensure its reliability and accuracy, while also preserving the rights of the individual and ensuring the interrogative and trial phases are equitable. (Parkinson & Khan, 2024).

Firstly, the legislation must be strictly limited to ensuring, that the algorithms used to collect and analyze forensic evidence are kept intact. The relevant authorities must establish strict statutory standards, to allow evidence obtained through artificial intelligence, especially the confirmation of the algorithm's accuracy, neutrality, and transparency. It is necessary to ensure transparency by reviewing and auditing the algorithms, that can reflect biases in the data used to feed the algorithms, which can lead to unfair and unjust results. On this point, multiple studies of legal and ethical nature have suggested, that conditions like those established in other countries (the United States and the European Union) should be implemented, where strict conditions are demanded, that make transparent the processes and algorithms, which comprise the criminal justice system (Goodman & Flaxman, 2017; Chouldechova & Roth, 2021). Some legal systems, including that of the United States, require ensuring, that algorithms used in criminal justice decision-making, such as risk assessments or sentencing, do not exhibit biases that result in disproportionately negative outcomes for specific demographic groups, which necessitates that the relevant laws are developed with specific, nuanced legal standards that promote fairness and equality.

Developing Legal and Technical Capacities & Improving Collaboration between Technical and Legal Experts

Using AI in forensic evidence needs detailed legal and technical preparedness, as these advanced technologies need to be well addressed, before they can be effectively handled in legal environments. But these transformations require the Saudi judiciary to be able to adapt, these requires intensive, sometimes designated, training courses for judges and lawyers, to teach them how to use these technologies, and the legal challenges that may arise when dealing with it. These types of training programs should include both technical aspects—such as exploring algorithms and data analysis—and legal aspects, including privacy, the permissibility of digital evidence, and algorithmic bias. The importance of such training cannot be overstated, as it ensures informed decision-making based on evidence from AI that is accessible, understandable, and observable by all parties in the judicial process.

For example, other countries have made some strides in incorporating AI into their judicial systems, that can be learned from. Legal experts in the United States are collaborating with technologists, in the field of criminal data analysis, particularly leveraging AI technologies in the context of criminal investigations, including the analysis of images and videos of criminals. Some U.S. states, such as California, have developed initiatives aimed at providing judges and lawyers training on digital evidence originating from AI (Binns, 2020). In the United Kingdom, AI has been integrated as part of investigative procedures, where lawyers are trained on how to analyze and interpret the big data of evidence as well as the interpretation to be done regarding criminal records from software (Bryson & Winfield, 2020).

In addition, collaboration between technical and legal experts, on a continual basis serves as an increasingly important aspect, when it comes to crafting workable solutions to legal and technical matters, within the criminal justice system. Proposals in France have already introduced professional, which programs to promote collaboration between the data scientist and the lawyer aimed at improving the use of AI in forensic evidence. These programs help increasing the understanding, between lawyers and technologists about the ways digital evidence should be treated, and how AI can be handled in a legal and ethical way (Goodman & Flaxman, 2017). Such collaboration is vital to developing technological solutions, that find the right balance between technological improvements in justice and the protection of individual rights, from the potential harms associated with big data and complex algorithms.

Likewise, a recent study in Indonesia (Afdhal & Suhra, 2024) stressed the role of the legal profession as a stakeholder in the use of AI in the judicial system. The researchers stressed the importance of training lawyers in the use of these technologies, to make sure justice is rendered. The involvement of technical experts in the legal process is not merely a passing novelty; it is essential in creating appropriate legal solutions, that accompany the employment of AI in judicial practices and requires ongoing collaboration by lawyers with technical experts. This model from Indonesia shows, how judicious efficiency can indeed be improved through continuous training for lawyers, promoting collaboration between the technical and legal sectors.

In this regard, it should be stressed that the effective development of legal and technical capacity, within the Saudi judicial system, must take place in close coordination between all relevant parties, including, but not limited to, the Ministry of Justice, judicial bodies, universities, and technology companies. This cooperation will not only improve the technical efficiency of the courts, but will also ensure a high level of protection of individual rights in the field of use of AI technologies, in the process of investigation and trial (Sabry et al., 2022).

Conclusion

Finally, this study explains that the use of AI technologies in the Saudi judicial system reflects a positive measure, regarding the effective and efficient advancement of the criminal investigations process. However, this effort presents a unique set of legal and ethical complications. It works with various stakeholders from the digital ecosystem, to help address and navigate the growing importance of technological development, and uses AI, IoT, and Web 3.0 technologies at work, generating insights from these technologies in the legal domain. Thus, when drawing comparisons with other legal systems, including that of the United States, which adopts the Frye and Daubert standards for determining the reliability of evidence, and the United Kingdom, which focuses on the rigorous examination of facial recognition technologies, it becomes clear that a comprehensive legal structure for the Kingdom is of paramount importance. These standards should include clear standards for the admissibility of evidence, requirements for transparency in algorithms, and mechanisms for assessing risks and biases. It is also suggested to develop special training for judges and lawyers on the use of AI in forensic evidence, while highlighting the need for protecting individual rights and privacy according to the tenets of Islam. Striking a balance between technological innovation and the protection of individual rights, while upholding Islamic principles, will be fundamental to an effective and trustworthy judicial system. This is in line with the Kingdom's efforts to implement principles of justice and protect rights based on the provisions of Islamic law and will promote public trust in justice.

Acknowledgment

Author of this Article would like to thank the Governance and Policy Design Research Lab (GPDRL) of Prince Sultan University (PSU) for their financial and academic support to conduct this research and publish it in a reputable Journal.

References

- Afdhal, A., & Suhra, A. M. (2024). The role of the lawyer profession in using artificial intelligence in the judicial system in Indonesia. *International Conference on Actual Islamic Studies*. <https://doi.org/10.1234/icaais2024>
- Al-Faiz, S., & Al-Juhani, M. (2020). The role of artificial intelligence in criminal investigations in Saudi Arabia. *King Saud University Journal of Criminal Justice*, 17(1), 44–58.
- Al-Saadi, M., & Al-Hamzi, F. (2022). AI in law enforcement: Saudi Arabia's adoption and challenges. *Journal of Emerging Technologies in Law*, 28(3), 211–225.
- Alshahrani, A., Dennehy, D., & Mäntymäki, M. (2021). Adopting artificial intelligence in the Saudi Arabian public sector: Preliminary findings. In D. Dennehy, A. Griva, N. Pouloudi, Y. K. Dwivedi, I. Pappas, & M. Mäntymäki (Eds.), *Responsible AI and analytics for an ethical and inclusive digitized society* (Vol. 12896, *Lecture Notes in Computer Science*, pp. 109–122). Springer. https://doi.org/10.1007/978-3-030-85447-8_7
- Alsharif, A. (2021). The role of artificial intelligence in Saudi criminal proceedings: Legal and ethical considerations. *Arab Law Quarterly*, 35(4), 452–476.
- Al-Tabari, M. ibn J. (1997). *History of Al-Tabari*, vol. 2 (M. P. Mahdavi, Trans.).
- Alghamdi, A. (2022). Scientific evidence in Saudi Arabia: Analyzing the challenges and proposing reforms. *Journal of Comparative Law Studies*, 10(3), 45–62.
- Alsamara, T., & Ghazi, F. (2024). The steady development of digital law: New challenges of artificial intelligence. Creative Publishing House. <https://doi.org/10.62754/joe.v3i5.3957>
- Albakjaji, M., & Almarzouqi, R. (2024). The dilemma of the copyrights of artificial intelligence: The case of Saudi Arabia regulations. IGI Global Publishing. <https://doi.org/10.4018/IJSKD.336920>
- Butt, J. S. (2024). The General Data Protection Regulation of 2016 (GDPR) meets its sibling the Artificial Intelligence Act of 2024: A power couple, or a clash of titans? ResearchGate. <https://www.researchgate.net/publication/384682777>
- Binns, A. (2018). *AI in the legal sector: A review of applications and implications*. Springer.
- Eubanks, V. (2022). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Frye v. United States, 293 F. 1013 (D.C. Cir. 1923).

- Howell, B. (2024). Regulating artificial intelligence in a world of uncertainty. American Enterprise Institute. <http://www.jstor.org/stable/resrep64560>
- Mansoor, M., Paul, J., Saeed, A., & Cheah, J. H. (2024). When mass meets prestige: The impact of symbolic motivations, inspirations, and purchase intentions for Masstige products. *Journal of Business Research*, 176, 114591.
- Howell, D. (2024). The Privacy Act of 1974. *The Federal Privacy Law Review*.
- Kuner, C., Svantesson, D. J. B., & Bygrave, L. A. (2020). *The GDPR and its impact on artificial intelligence*. Oxford University Press.
- Latham & Watkins LLP. (2024). In-depth: Artificial intelligence law in Saudi Arabia. Lexology. Retrieved from <https://www.lw.com/admin/upload/SiteAttachments/Lexology-In-Depth-Artificial-Intelligence-Law-Saudi-Arabia.pdf>
- Papagiannneas, S., & Junius, N. (2023). Fairness and justice through automation in China's smart courts. *Computer Law & Security Review*, 45, 105897. <https://doi.org/10.1016/j.clsr.2023.105897>
- Parkinson, S., & Khan, S. (2024). The role of artificial intelligence in digital forensics: Case studies and future directions. *Assessment and Development Matters*, 16(1), 42–47. <https://doi.org/10.53841/bpsadm.2024.16.1.42>
- Wang, N., & Tian, M. Y. (2023). "Intelligent justice": Human-centered considerations in China's legal AI transformation. *AI and Ethics*, 3(2), 349–354. <https://doi.org/10.1007/s43681-022-00202-3>
- Wang, R. (2020). Legal technology in contemporary USA and China. *Computer Law & Security Review*, 39, 105459. <https://doi.org/10.1016/j.clsr.2020.105459>
- Zanfir-Fortuna, G. (2020). The European Union's approach to AI and data protection. *International Journal of Law and Information Technology*, 28(1), 47–68.
- Garvie, C., Bedoya, A. M., & Frankle, A. (2016). The perpetual line-up: Unregulated police face recognition in America. Georgetown Law Center on Privacy & Technology.
- Fussey, P., & Murray, D. (2019). Independent report on the London Metropolitan Police Service's use of live facial recognition technology. University of Essex.
- Shura Council. (2021). Report of the Committee on Judicial Affairs Regarding Artificial Intelligence Technologies.
- Saudi Data and Artificial Intelligence Authority (SDAIA). (2023). AI Ethics Principles. Retrieved from <https://www.sdaia.gov.sa>
- United States Department of Justice. (2020). Fourth Amendment: Protection Against. National Institute of Standards and Technology (NIST). (2021). NIST framework for digital evidence and AI systems in courtrooms. Retrieved from <https://www.nist.gov>
- National Institute of Standards and Technology. (2021). Digital evidence and artificial intelligence: Evaluating the use of AI systems in courtrooms. Retrieved from <https://www.nist.gov>
- Australian Law Reform Commission. (2015). Evidence Act 1995: A legal analysis of digital evidence in Australia. Australian Government. Retrieved from <https://www.alrc.gov.au>
- UK Government. (2018). Data Protection Act 2018.
- The Quran, Surah Al-Hujurat, Ayah 12.
- Ibn Sa'd, M. (2001). *Al-Tabaqat Al-Kubra*, vol. 1.
- Muslim, A. (1998). *Sahih Muslim, Book of Hudood (Punishments)*