Journal of Human Security | 2025 | Volume 21 | Issue 2 | Pages 77-83
DOI: https://doi.org/10.12924/johs2025.210212
ISSN: 1835–3800

Journal of Human Security

Research Article

Smart Criminal Justice: The Smart Police Station as a Model for Legal Innovation

Dr. Youness Nafid [1*], Sara Joraiche [2]

[1]Department of Law, College of Criminal Justice and Criminology, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia.
Email: YNafid@nauss.edu.sa
[2]Economic, and Social Sciences, Faculty of Legal, Chouaib Doukkali University in El Jadida. Trainee Lawyer at the Beni Mellal Bar, Morocco.
Email: sara2joraiche@gmail.com

***Correspondence:** YNafid@nauss.edu.sa

Submitted: 20 September 2025 | Revised: 27 October 2025 | Accepted: 25 November 2025 | Published: 30 December 2025

Abstract: This study critically examined Smart Police Stations (SPS) in the Gulf and Europe. The methodological and cross-jurisdictional approach examined the policy and protection of SPS systems with rights using policy documents, legislation, and performance material of the acquired success. The results show that Gulf countries have done well in digital policing, efficacy, and institution integration. These triumphs were achieved by navigating a range of evolving legal and ethical challenges, particularly regarding privacy and responsibility issues. Europeans legally established principles based on openness, equity, and procedural justice to model ethical technology use. This is extrapolationally difficult to other regions and does not indicate local suitability without contextual adaptation.

Keywords: Smart Police Stations (SPS), digital policing, Smart Criminal Justice.

1. Introduction

The rising use of artificial intelligence (AI) in institutional contexts can signal a new social, economic, and legal epoch. A specific operational plan guided AI and predictive analytics automation. Second, new technology simplified work and opened new opportunities. Along with equity, it raised privacy, responsibility, and other concerns. In criminal justice, AI-related thoughts and solutions replace civil order system reports, demonstrating two-sidedness.

One significant example of this trend is the Smart Police Station (SPS), a computerized facility that can deliver policing, legal, and administrative functions with minimal human interaction. A speedier public service is promised by the SPS model since latest technologies like digital identification verification, real-time data analysis, and automated case management boost accessibility and workability. First-movers like the UAE and Saudi Arabia have integrated SPS initiatives into their digital transformation strategies to modernize their administrations Mega issues should be eliminated. Reserve creators and experts are concerned about technology discrimination, whether granting exterior-facing personal rights to cyberspace is the right action, and whether automation decisions can be made with a broadly open-minded. Efficiency and effectiveness are difficult subjects for technology innovation and good administration. Countries seek to provide transparent, truthful, and effective systems and procedures, as well as trust and security, for their inhabitants. Global uncertainty has increased. The EU is right-oriented (e.g., the EU Artificial Intelligence Act), China is system thinking, and the US is spyware and active-police, [1].

Smart Police Stations, a Smart Criminal Justice system case study, will be included in this project. The Saudi and Emirati international research paradigms are discussed and evolving. It links all international norms to fair trial, privacy, and accountability. The report requirement bridges the gap between current security practices and legally binding international standards. Finally, the research would contribute to a trade-off because the efficacy of law compared to technology would expand digital justice literature and help policymakers balance the players of the technological revolution [2].

1.1 Statement of the Problem

The rapid development of smart criminal justice in policing, legal, and judicial arenas is linked to data systems and AI. However, accountable deployment still puzzles legal academics and practitioners. Comparisons always indicate that results are unequal and the governance and legitimacy system is unclear, especially when rights protection is altered by automation. Algorithms improve reporting, triage, and analytics but also introduce bias, obscurety, and due process issues. Accountability is complicated by technical models, data administration, organisational processes, and human control. To accomplish justice, explainability, and proportionality in smart policing, contextually applicable legal protections and open evaluating procedures are needed, [3].

Public faith in smart criminal justice systems is based on fairness and AI's temporary success. These barriers are especially evident in the smart police station model, which delivers unified, noncontact services, but a strong government should reduce dangers and protect rights. The lack of a defined, empirically verified design and audit concept for smart police stations that ensures legality and legitimacy remains a major barrier. Current studies have not harmonised accountability concerns across the system lifespan, including data governance, operational controls, and remedials. Regulatory studies advocate the risk-based strategy, but institutional roles and enforcement are lacking. In the fast-paced technological innovation environment, difficult challenges remain about how to implement control and transparency.

According to empirical research, AI in policing was traditionally relied on the existence or absence of its pure and simple findings. However, technical efficacy and perceived validity will always vary. The adoption and enforcement of algorithms has found that eliminating prejudice in many settings is difficult, especially for vulnerable populations and other application scenarios. Onlookers have called for a rights-based, fair, and auditable paradigm based in Saudi Arabia. Effective bias reduction, institutional responsibility, and binding transparency norms will characterize future functioning. After building trust and proving everything is well, resources can implement risk-based governance. Major changes that unite legal validity and social needs are needed to achieve smart criminal justice, [4].

1.2 Study Significance

This work contributes to Arabic smart criminal justice literature, which is understudied in regional academic literature. The theoretical and regulatory surroundings of the Smart Police Station (SPS) are placed in digital justice. Analysing artificial intelligence in police involves ethical and legal challenges such algorithm bias, openness, and accountability. Digital change in criminal justice and security in the UAE and Saudi Arabia is also

examined in the report. The study concludes with practical advice to help politicians reconcile operational performance with basic rights and strategic implications for other smart cities looking to adopt the same approach.

The work is relevant to the AI debate and digitalization of natural punishment. This testing of the analysis utilizing Smart Police Stations as a unique analytical model fills a vacuum in local and global literature on technology innovation, legal protection, and procedural justice. The focus on comparative study and the creative Saudi and Emirati model show how a jurisdiction is implementing AI-driven systems without considering accountability, privacy, and basic rights concerns.

It merges theoretical study and practice to measure intelligent police platforms' compliance with international law principles including the right to a fair trial and due process, making it relevant. The study emphasizes operational efficiency and legal validity, unlike the prior study, which focused on technological effectiveness or theoretical regulatory difficulties. The work informs scholarly discussion and policymaking by assessing the merits and downsides of existing digital policing formats to establish the best balance between innovation and monitoring.

Additionally, the paper can offer practical advice to legislators, law enforcers, and institution managers who want to implement smart justice programs. This will strengthen theoretical understanding and help build strong governance structures, boosting public trust in the long-term digital transformation of the criminal justice system.

1.3 Study Objectives

1. To explore the legislation and intellectual foundations of smart police stations and smart justice systems.
2. To know how to create the smartest police stations most useful in the world.
3. To understand if the stations adhere to the requirements and conditions of the international law, which presupposes a fair trial.
4. To develop a legal and ethical reason as to why AI ought not to be used in law enforcement.
5. In order to provide suggestions to help the fair and just use of technology in the criminal justice system.

1.4 Study Questions

1. What impact has the Smart Police Station had on maintaining peace and upholding the law?
2. How have the international experiences of Dubai and Riyadh affected the delivery of timely and efficient police service?
3. Are such stations complying with international laws like the International Covenant on Civil and Political Rights that guarantees people their right to a fair trial?
4. What are the legal and ethical issues involved relating to smart policing, discrimination, mass surveillance, and information security?
5. What shall the law say about the use of Smart Police Stations so that they may be safe?

2. Literature Review

2.1 Comprehensive Overview

The current study (2023-2025) critically improved criminal justice AI understanding, including predictive policing, transparency, accountability, regulatory design, and public trust. Recent predictive police research has focused on fairness and prejudice, linking algorithmic inequalities to social and institutional legitimacy. Organize bias causes, mitigation techniques, and evaluation metrics, shifting the topic from basic concepts to quantitative protective measures. Eight sociotechnical issues connected to algorithmic policing, including traceability, explainability, institutional embedding, and cross domain contestability. He agree that AI accountability is complicated and requires legal, technical, and administrative considerations. Cheong ,Goh [5] analyzes how transparency as a state of social legitimacy might maintain public acceptance of algorithm procedures. Legal scholars view the European Union AI Act as the new frontier of legal AI policy, as they argues that it is the key to rights protection and the need to innovate when applying AI to law enforcement.

The Gulf-region studies have also shown rapid policing institution digitization. He examines an Abu Dhabi Police virtual reality training centre, whereas he analyses UAE police intellectual capital indicators. They value operational innovation and managerial performance over rights-based appraisal. Public trust also determines legitimacy. He argue that institutional trustworthiness determines public opinion about AI-enabled facial recognition in law enforcement, while argue that it is the foundation of AI governance and affects compliance and acceptance. Interesting prospect. Only the digitalization of police agencies, which is underway, can change occupation in the Gulf. He discusses Abu Dhabi police virtual reality training center research. Performance-based, operational, and rights-based innovation are their goals. Last but not least, society must be credible to itself. The scientists found that self-emotional attitude toward an organization affected their impression of police department AI-based facial recognition. The message reminded readers that trustworthiness and trust provide acceptance and compliance, hence AI is managed by them [6].

2.2 Thematic Analysis

Bias and Legitimacy. Predictive policing will worsen systemic issues without justice rules. The power of justice must be stratified by institutions, processes, and technology [7]. They found that statistical fairness, like equal chances or demographic relaxation, must be in law. Predictive policing can use fairness criteria to reduce prejudice and improve findings.

Transparency and Accountability. Along with openness, accountability is a common topic in algorithmic policing. Transparency includes explainability, procedure, and auditability, per [8] lists eight interrelated accountability concerns, from traceable data provenance to redress procedures. define accountability as the development of agents, rules, and monitoring regimes that must be dynamically interactive between rules and actors. These contributions regard responsibility as more than a sociotechnical ecosystem notion.

Regulatory Responses Sachoulidou [9] states that the AI Act initiates European criminal justice AI discussions. Her work focuses on preventing biometric misuse (e.g., in places of worship), categorizing hazardous technology, and creating legally oppressive measures for due process. The Act did not discover the law, but it can be used to locate other sites, especially in the Gulf, to balance creation and fundamental rights.

Regional Deployment (Gulf). It is unnecessary to discuss human rights, but a brief explanation of the Gulf region will help visualize AI in institutions. The writers repeatedly highlight the Abu Dhabi Police, their performance, and capacity training in fully designed immersive virtual reality training accidents, [10]. Intellectual capital is crucial to the UAE police force's growth due to managerial innovation. However, the two documents lack human rights norms like challengeability and justice.

Public Trust. People's trust determines AI-powered police credibility. The authors found that institution credibility regulates the legality of AI face recognition in enforcement, and the larger the system, the less legitimate the subject matter. They support the governance system's implications, highlighting trustworthiness and trust as vital to AI governance in all three scenarios. All of this shows that trust is vital to the social acceptability of law enforcement AI research.

2.3 Comparative Analysis

Disputes and agreements can have ampere-longitudinal lines. Justice and quality service are known to assist in many situations. In contrast, Gulf research focuses on performance management and organizational innovation, while EU publications address the issue of enforceable rights and recourse. A fissure in the laissez-faire institutional culture has been blamed for competency concerns in Gulf operations and adoption of European due process. Comparing multiple measurement methods is tricky. Both EU and Gulf studies demand efficiently coded accountable and descriptive management indicators. Comparing study trust. The institutions were unsatisfied with their efficiency and innovation, so only trust could persuade the public.

2.4 Integrated Synthesis.

The data show that algorithmic bias affects equalism, which does not exist on the open, accountable, and binding governance platform. Rights-based rules include the EU AI Act, which ensures fairness, openness, accountability, and confidence in criminal justice AI use. Gulf is creative in management and technology and integrating due and accountability credentials. Trust is favorable to a larger bridge because third-world toleration should be founded on confirmable openness and responsibility, not efficiency [11]. Future studies should use longitudinal and mixed-method research to define fairness indicators, accountability environments and their quantitative consequences, and culturally informed trust scales. Incorporation would bring order to Saudi Arabia and the UAE, making smart police stations less ambitious.

2.5 Research Gap and Current Study Objectives

The introduction of the Smart Police Station (SPS) in the Gulf via use of new technology can be objectively evaluated. Descriptive methods of innovation are implemented. Nevertheless, the nature of rights is not an

issue of contention. Longitudinal mediators of the trust concept have been applied in sparse studies, which consider the use of Arabic culture, but longitudinal mediators of trust can be applied to time in general. The deficit (i) will be compensated by (i) operationalization of accountability and fairness measurements in the SPS, (ii) development of standards of legitimacy and trust in the Arabic context, and (iii) development of its substance-specific legal standards according to the legitimate EU norms, taking into account the realities of the Gulf organization.

3. Methodology

This study used an analytic comparative technique to evaluate how Smart Police Station (SPS) become a modern Smart Criminal justice paradigm. The proposed research design achieved the study objectives by combining qualitative content analysis, doctrinal law assessment, and cross-jurisdictional case comparison. The data included peer-reviewed academic sources, policy documents, legal frameworks, and official reports from 2021-2025 on empirical findings and norms in the UAE, Saudi Arabia, US, China, and EU.

Starting with the EU Artificial Intelligence Act and specific policies that drive digital change in criminal justice systems, the examination will examine legal tools of interest. The research has been able to completely evaluate SPS's conceptual base while defining technological, legal, and operational aspects of diverse jurisdictions. The comparison examined SPS system deployment, monitoring, and responsibility mechanisms, focusing on the Emirati and Saudi versions.

In the assessment model, procedural fairness, privacy protection, and accountability were used as indicators of technological innovation and legal rectitude. Analytical triangulation was used to ensure validity by claiming statutory texts, recording best practices, and thematically synthesizing qualitative information.

4. RESULTS

Most overseas police stations have excellent fittings, including Emirati, Saudi, American, Chinese, and European models. The paper discusses the rise and development of smart policing programs, the level of services provided, the unique characteristics of each model, the critical analysis of their operating performance, the obstacles and limitations to their execution, and the regulations and checks that protect such systems. The main goal is to assess smart policing's operations and legal-ethical framework in diverse countries. The researcher compares empirical facts, policy formation, and legal rules, as well as learning points and recurring challenges. These quantitative indicators combine with qualitative observations to provide multidimensional information. The findings are believed and presented:

4.1 The Concept of Smart Police Stations (SPS)

Smart police stations (SPS) pose a new format paradigm of international security where the purpose is to enhance the effectiveness, accessibility, and visibility of the police. The SPS projects are integrating the artificial intelligence (AI) and Internet of Things (IoT) in order to get access to service and trust for more and more varieties of circumstantial events, The selected critical overview of the international best practices in SPS, that is, the Emirati model, offered in this paper is supposed to examine strategic objectives, the nature of operations, and the digitalization of the problem of privacy and data control and trust in authority [12].

4.2 The Emirati Experience: Dubai Smart Police Station (SPS)

Dubai's evolution into a global and regional digital development leader includes introducing the SPS model. Dubai is part of the Smart Vision, a complex of new law enforcement and digital governance principles that must be more productive, sustainable, and mindful of residents. This force was the first to employ technology as an innovation and confidence arm to citizens and introduced a prototype of automation and accessibility with SPS facilities, leading to these new Gulf police standards.

Dubai SPS services are holistic and inclusive. Its SPS stations are open 24/7 in multiple languages so residents can report lost items, make complaints, and receive permits and other indirect services from this police force without having to speak to a person. Dubai's smart infrastructure improves functionality, and biometric checks and digital identity technologies make users more comfortable. Emirati SPS values technology. Facial recognition, case management, predictive analytics, personalization, and operational efficiency are possible with AI. The absence of paper operations and environmentally conscious building design raise sustainability awareness in Dubai, so digital policing may serve environmental and urban governance purposes. Performance indicators have improved with SPS adoption, according to empirical assessments. Wait times are shorter, case processing is more accurate, citizen satisfaction and trust in policing organizations rise. Privacy, ethical boundaries of AI-powered surveillance, and data control have also been disputed. The systems of monitoring are also evolving, but experts say sustainable legitimacy will be predicated on governance openness and legal protection of individual rights [13].

4.3 The Saudi Experience: Digital Transformation of Public Security

In Saudi Arabia, Vision 2030 affects the transformation architecture framework. It aims to strengthen institutional foundations. This differs from managing secure, efficient, and friendly state services for individuals. In this method, vision statements presume national pride, international competitiveness, and operation competency are the main reasons people develop new technologies. The administration has improved accountability and responsiveness by thoroughly transforming the Ministry of Interior to make law enforcement and justice world-class.

Integration of e-government interventions like Absher and Tawakkalna, which offer crime and traffic reports, permits, and court applications, has also marked a turning point. They are crucial to Saudi Arabian and Gulf organization citizenship and modernization. AI, IoT, and real-time data can reduce red tape and streamline government procedures, making it more accessible. The latest publication uses these technologies [14].

The digital revolution in Saudi Arabia has made the government more interconnected, supplied information security circumstances, and is likely to spend more on computer virus defense and cloud computing. Each of them helps the security industry, lubricated with nakedness, remember how ill-strotious it is, facilitating various computer usage techniques and keeping their firm afloat [15]. The important Saudi public security reform changes the institution's operation and allocates privacy and human rights according to international norms.

But there are difficulties. The only thing that could halt this trend was law enforcement's reluctance to change. Digital infrastructure and access service disparities between towns and villages exacerbate the digital divide. Personal privacy, algorithmic peak-based decision-making, fair service delivery, and other challenges remain important to society. To partially address these problems, money is not the only solution. It will also require increased transparency, accountability, and an open state agenda.

4.4 Other International Experiences with Smart Police Stations

4.4.1 The American Experience

The US is partially successful in this area, yet the police stations are not fully automated with AI and analytics yet. Predictive analytics, facial recognition, and drones are used by the police sometimes in the US, though. The algorithms that predictive policing uses are based on data regarding previous crimes and their locations to deploy patrols to areas that are believed to be less secure. People use drones to contain crowds, conduct aerial inspections and save lives. Face recognition could easily recognize an individual and can be applied in an inquiry. The study warns, though, that algorithmic policing can also help to strengthen systemic inequalities, including racial and ethnic ones, and is a matter of concern that must also occupy a central place within the rights and legitimacy approach Mass monitoring, privacy and split power are not being enthusiastic about the US decentralized system of law enforcement due to constitutional reasons. According to the researchers, such tools can be helpful due to strong legal regulations, accountability and the uniqueness of technology.

4.4.2 The Chinese Experience

China is working towards an entirely different model and is wide-rangingly deployed in its Smart City concept. The Sharp Eyes project determines e of 24/7 coverage in the city and in the countryside with the help of analytics based on artificial intelligence and millions of cameras Cities such as Shenzhen, which have integrated governmental structures, have been built, bringing together the data gathered by different authorities that secure law enforcement in real-time and process cases fully automated, and community portals have been examples. Besides, results of the Policing Clouds projects show that China has offloaded the core operational aspects of policing into the cloud-based system and centralized system and increased the solutions of analysing and heating the debate on access controls and proportionality. Although the enhancements in

capabilities can be deemed as necessary, researchers also point out the fact that they are also coupled with the growing discussion on the issue of privacy, transparency, and the need to hold anyone accountable.

4.4.3 The European Experience

As part of the European Union, the risk-based regulation is a strategy via which the hoped-for anticipated artificial intelligence legislation is anticipated to be stringent in comparison to the deployment speed plans. The Act specifically bans or restricts the implementation of some enforcement uses, including facial recognition in the business environment, and conditionally grants potentially dangerous AI systems a very stringent transparency and responsibility set of situations. According to some of the findings of the research, the EU framework has been offering a governance structure emulated by other jurisdictions that must be clarified and overseen and repaid. Such options, which can be viable, are listed and these are experimental AI-controlled border control programs or an online police-related site that should be open and accountable. Lastly, it includes the possibility to integrate the intelligent nature of the police technology into an effective human rights and democratic context of the security environment.

4.5 Global Challenges in Smart Police Station Implementation

These self-copying deformities of SPS are so predictive of the world that they have made it ineffective and socially unacceptable in every niche of the globe. Similar to the technical counterparts, SPS deployments have robust data pipes, system integration centers and a lifecycle control mechanism in the models. They are in control in radiance of organizations regarding training, policy, andculture change. According to the research about algorithmic policing, accountability is characterized in terms of data provenance and explainability, institutional responsibility and redress procedures and addresses technological, organizational and human accountability. The problems connected with the design demand an auditable design-based approach compared to the design architecture. Considering the heightened SPS activities, privacy and data safety are becoming an issue. These duties have now included sensors that operate everywhere, real-time analysis and betic or computer vision problems. The fear that non-transparency in automated rule-making may carry adverse consequences on the individual and social well-being is one of the trend lines prevailing in the area of legal and ethical writings. This is since there is only change in laws as well as system governance if it is open and accountable, being part of governance. Automation can affect the due-process rights, especially in a criminal justice system context, the presumption of innocence, the capability of controlling the output, and in what situations automated reasoning can be subjected to acceptance. To that extent, preceding work with specific endorsement and license and diminished willingness and an accessible network of accredited access is approached. The government is also based on the links between SPS and city data lakes and identity sanctuaries. Privacy and data protection seem to be treated as more important these days due to more operations by SPS. It has also expanded to include sensors that function remotely, real-time analytics, and bit-level or computer vision issues. The fear of the absence of transparency in automated rule-making instruments poses a threat to the welfare of individuals and society: currently, it is the ultimate and pressing issue in the realms of law and ethics articles. It is forced to do so because laws and regimes may evolve, unfortunately, unless they are free and open, which is an aspect of authority. There is a possibility of automated procedure affecting the rights to due process, especially the criminal justice system, the presumption of innocence, the ability to regulate the output response, and the situations when automated reasoning is acceptable. To that end a stronger reliance between an encouragement of forced labor with actual power and license and an absence of willfulness plus offsetting vivacity is provable. Utilizing SPS allows the government to approximately locate sanctuaries by maintaining communication between data lakes towards cities, [16].

Fairness and prejudice will never take it easy. Long-term predictive policing research has been used to illustrate how algorithm systems with no specifications regarding what is becoming unfair and what is staying fair can be deployed to lean more towards historical injustices as well as magnify them). It can happen as a result of distortions of the facts by an individual or just the mere coincidence. The issue of measuring and monitoring fairness within a specific application at any point in time would be possible, though active patrol division, risk triage, incident routing, and SPS applications (active patrol division) should not anticipate functioning without the aforementioned issues. Equity does not assume anything like the one that has been actually new and experimentally verified as an aspect of SPS techniques but instead is nothing but an illusion. Things of governance and legislation further worsen the situation. A comparative analysis makes the assumption that incapacitance in the exorbitation of the substantiation of innovation and essential rights will not be fetched and identifies as factual that hard author accountability, audit trails, finding influence, and autonomous control are critical decision-making specifications of the SPS that are subject to review and discussion. Some enforcement practices have been more threatening than ever in areas where the EU rules have been implemented. The applications will further be interrogated, vetted and revised. Regulations can be shameless; however, the relationship between the technological piece may be inactive, which creates the unequal enforcement of the thought and inequalities in the volumes of requirements within the real world. Finally, the validity of the SPS can be anchored in the few individuals that acknowledge it. The results of interdisciplinary studies have shown visible accountability, institutional integrity, and substantive transparency to be applicable to trustworthiness and confidence and not efficiency. When it has been improved in the indicators of service, then it's tabula rasa because people have no bodily method of seeing, inquiring, or challenging what is arbitrated by computers. The governments and the affected communities, the civilians of the societies, have to wage war collectively to gain their trust. Embarking on intensive evaluations through which the parameters of fairness, accountability structures, and the result and seeing through time are measured are also worth attaching to them.

5. Implication.

In the current SPS, an integrated program consisting of (i) (i) fairness-by-design with longitudinal verification, (ii) end-to-end accountability (between data provenance and redress), (iii) rights-protective regulation alongside high-risk safeguards, and (iv) trust-building by transparent and participative targeted oversight is needed.

6. Comparative Critical Discussion

A review of the foreign experience while implementing smart police stations will show numerous trade-offs, which have occurred between innovation, legislation, and rights preserved. The modernization and digitization process is no longer slow in Gulf countries and thus brings efficiency and contentment amongst citizens, but the security issue still exists. Such projects as Sharp Eyes and Police Cloud have been viewed as a concern of large-scale efficiency in China because of transparency and civil liberties. However, the issue of structural deficiency is prevalent in the American system even with the level of high-technological development since there is a lack of decentralization, and the argument of equal application and due process remains a problem. The AI Act is a legislative framework of the European Union, also concentrating on the transparency and human rights in the governance of the legislation, [17].

We not only engage in imitating the information that each of the instances contains, but we focus on the similar tension: the benefit of efficiency versus the safeguarding of the rights, technical advancements versus the stability of the rules, and the ambition of a manager versus the issue of legality. The exposure to the diverse cases of situations as well as the universal significance of technological innovation combined with transparency, accountability and excellent legal teaching. In order to achieve long-term legitimacy of AI-assisted law enforcement, regardless of the jurisdiction, strong shields should be found with innovation, [18].

6.1 The Need for a Legal Framework for Smart Policing and the Legal Safeguards That Must Be Observed

6.1.1 First Requirement: Towards a Comprehensive Legal Framework for Responsible Use of Smart Policing and the Challenges

The increased use of smart police technology outlines the significance of a diverse and integrative system in legislation that promotes transparency, accountability, and respect for privacy rights. The aspects concerning how artificial intelligence analyzes information processes, biometric identification, and digital services in the fields are not specified, which adds to the probability of privacy breaches and the loss of responsibility. One of the most critical aspects regulating the collection and use of sensitive personal information, defining the parameters for using endangered AI, and introducing measures for liability control and remedies. To minimize the problem of opacitance and abuses, comparative research has demonstrated the need to codify responsibility in the shape of the legislative tasks concerning explainability, auditability, and human control, [19].

6.1.2 Towards an Arab Legal Framework for Smart Police Stations to Protect Electronic and Smart Data

Long strides have been taken in the Arab world. The Personal Data Protection Law (PDPL) in the United Arab Emirates under federal regulations is decree number 45, 2021, which restricts the authorization of sensitive information and protects the right of the individual. In Saudi Arabia, the responsibility towards the enhancement of the degree of digital governance was defined by a Personal Data Protection Law (which was enacted in 2021 and revised in 2023), making it a duty of not only the population but also the business sector. Such standards create a legal framework for protecting the electronic data used in the course of smart policing, but further industry-specific laws to address the issue of AI surveillance and automated decision-making are necessary. Scholars emphasize that the necessity to address Gulf-specific challenges, especially those that are related to the data flow beyond the borders and the accordance in the jurisdictional interoperability, is paramount, [20].

6.1.3 The Need for Unified Regulation of Smart Policing in the Context of International Security Cooperation

Since the World's regulators were at differing levels of maturity, there was a possibility of creating homogenous standards through by a common convention organized by the Council of Arab Interior Ministers. With such an agreement, legal foundations of sensitive data processing would become official, lay the regulations concerning the enforcement of legal justice of highly risky AI in place, and pave the way to establishing the norms of data transmission between borders. It also needs to be subject to an independent judicial or administrative review that will make it more accountable, as well as provide the trust of the populace, [17].

6.1.4 Benefiting from Other Global Experiences

The benefits of the Arab region could be in comparative modelling models. The broadest risk-based regulation of the European Union is the AI Act that categorizes AI and demands transparency and documentation, or the human oversight of high-risk applications of AI, such as policing. In addition to the AI Act, the GDPR level of data protection is another global standard that puts an accent on the right protection and reasonable use. The data-governance model of Shenzhen is related to the advantage of inter-agency interoperability but also to the issue of proportionality and accountability in China. When applied to Arab countries, the combination of GDPR-improved protection and high-risk obligations founded on the AI Act can result in efficiency and rights realization. The need to possess legitimacy in the conduct of independent review, the regularity of auditing, and transparency is among the things that are taught, [21].

6.2 Second Requirement: Legal Safeguards That Must Be Observed and Their International Basis

6.2.1 Key Legal Safeguards

The legislative and institutional measures constitute some of the legal protection measures used in smart policing scenarios that ensure accountability, fairness and adherence to the basic rights. The study of answerability, audits, and redress mechanisms is also anticipated in the field of algorithmic policing since the latter must be acted upon by the mentioned means as well. The fundamental principles of contemporary criminal justice systems still embrace an upholding of privacy, equal treatment, and the right to trial by fairness. Studies describe the reasoned reasons why integrating justice into artificial intelligence technology and the legal definitions may not be transformed into technical quantifiable standards and could be challenging. This particularly invasive use, especially regarding privacy issues, means that the law should restrict the available scope against which biometrics and facial reconnaissance could be applied, laws must be open to some transparency, and the opportunity to revise the automatic conviction ought to be afforded, [22]

6.2.2 International Legal Foundations

Some of the basic rights of international law are the right to equality before fair tribunals, the right to hearings in the open, and the right to protection of privacy that is resolute. The European Union AI Act can be viewed as one of the most innovative documents in its orders, as it practices a risk-based policy and establishes any legal requirement that may be given to risky AI systems that are being employed by law enforcement. Further, the protection of personal data is strengthened by the right of the citizens to access, rectify and object under the general data protection regulation (GDPR) in addition to the protection of citizen rights [23]. The principles are universal solutions that the application of artificial intelligence in the legal system must imply responsibility and defense of rights necessarily.

6.2.3 The Need for Enhanced Safeguards in Smart Policing

Scientists present their argument that human control must not be left regardless of which form of AI-based court judgment is reached, and individuals must be informed to explore the logic behind the algorithm and exhibit how the decisarrived ate to its conclusion. The three main points that should be better addressed to the protection measures are tougher restrictions in the biometric surveillance, procedural security, and external audits. According to the comparative analysis, care must be taken so that no biased outcomes are used and that there is the possibility of the population keeping its trust [24].

6.3 Practical Examples from International Experience

The numerous examples of AI being used to view law enforcement are elucidated using actual life examples. According to recent EU research, the current coverage of the AI Act on the science behind explanation and the risk appraisal is contributing to the secrecy of the algorithms. The population would be crushed and given an opportunity to become legitimate when it comes to face scan legislation [25]. Although the process can be expedited in digital courts, the European ideas of advocating wider judicial reform still insist on the deployment of human judges. It is also an example that the fully independent court system is hostile regarding morality and legality [26].

7. Discussion

7.1 Interpretation of Results

The research achieved its objectives by looking at the application of Smart Police Stations (SPS) in some legal jurisdictions. Procedural justice is deemed to be an important feature of transparency and accountability, and an analytical and practical gap in the Gulf and European context was discovered [27]. Digital governance integration he was the feature of the Saudi experience, and the Emirati approach ensured that there were sufficient efficiency and institutional innovations. The European Union AI act on the other hand, introduced a stronger regulation, which emphasized more on algorithmic fairness, legal responsibility and rights laws. In both cases, also, it was determined that there were recurrent infringements of privacy and a lack of consistency in the exercise of the right to a fair trial that weakened social trust and that, in each case, technological changes had significantly surpassed the protection of the process, The stepwise listing of ethical and legal issues, alongside the significance of licensing, the option of opting out of procedures, and laws regarding practices with the digital data, revealed the existence of algorithmic bias, the lack of data protection, and the issue of spreading monitoring on a mass scale, [28]. Furthermore, different jurisdictions lack standard norms of operation, and hence, it is difficult to provide fair and equal justice.

7.2 Theoretical and Practical Implications

The research results complement legitimacy theory because they show that not only efficiency but also transparency and enforceable accountability define the extent to which legitimacy theory presupposes that the organization should require algorithmic policing in the long run. Evidence of the mediating role played by institutional trust had also supported it: the only difference was that it had been the public trust on which visible protection and redress mechanisms, as opposed to the services, had been set up rather than improvements in services exclusively that was being supported. The findings have inspired high-risk AI application regulation by the prescription of sector-specific legislation, which ensures the data and vendor contracts are effectively controlled by an independent body and data governance in reflection of the best practices in other countries. They having fairness validation should be the priority in professional practice, and the outcomes provided by AI must be artificial and verifiable, and the usage of the big data-gathering technique should be confined to non-legal operations. The strategies to be implemented as priorities in intervention must prioritize regularity in the monitoring of fairness, the incorporation of integrating supervising mechanisms, and embedding trust within specific communities due to their vulnerability to simplify the chances of the algorithmic bias proving to be detrimental. The next element that was described by the research concerns the need to introduce cross-sector collaboration between developers of technology, legal experts, and police to be able to implement ethics in AI structures.

7.3 Methodological Insights and Limitations

A wide jurisdictional survey of policy, empirical and legal evidence was made in this paper, where there was an immediate resemblance on the functioning outputs of the policy in parallel with dissimilarity across regulatory maturity. The advantage of the strategy is that it offers the overall scope of prominent international SPS paradigms and addresses the issues, which can jeopardize the state sovereignty, including the dependency on the vendor The primary weaknesses are the use of secondary sources, the potential absence of explanations of the civil society opinion on the problem of the system, and the limitation of the sample, which is explained by the expanding scope of the studies of the Gulf region. It shows the significance of the empirical study that there is a lack of direct qualitative data on the fairness and trust measures. Nevertheless, the gathering of many sources of data provided a sophisticated and situational analysis.

7.4 Similarities and Discrepancies

The latter investments in digital assets are now permitted to be more effective due to cross-border investments. However, the difference in privacy and its rights and fulfillment is occasioned by institutional, cultural, and legal factors. European ones are more explanatory and can be argued out use more ameliorative and less transparent systems in the Gulf. The assessment does not remain the same since the rights-based measures and the measures of success do not necessarily coincide. The comparative analysis is difficult to do due to the situational circumstances. These are civil society lobbying and people's reactions to surveillance. These factors also cause the differences in the trust of the public [29].

7.5 Integrative Conclusion

The work builds the field to provide an experimentally verifiable and modifiable template to the responsible SPS implementation. They must include built-in mechanisms that take into account sound legal transparency, end-to-end accountability and fairness by design. The longitudinal, mixed-method research designs can be used in future studies to ensure that the context-sensitive signs of fairness, checking-out mechanisms, and devising the willpower accountability actions exist, based on the realities at the regional level. The gap in knowledge that is debatable through the report is that the bases of operation novelty area are considered together with the widely acclaimed international best practices with practical suggestions to the policy makers and praxis enthusiasts in the dynamic setting of smart policing. Finally, this tactic is important when implementing future deployments that can ensure the generation of societal confidence and the addition of social advantage over the long term.

8. Conclusion and Recommendations

8.1 Conclusion

The Smart Police Stations (SPS) concept, its timely adaptation, its efficiency during work, and the various legislative frameworks through which it was informed will all be critically examined in this essay. The important findings are that even though the Gulf countries have revealed high efficiency and technological development, success is usually accompanied by the lack of legal protection and inequality of regulation enforcement. The European models, in their turn, have pegged the standards of procedural justice and institutional trust at a higher level and are more interested in the responsibility, transparency and safeguarding of rights as reflected in the EU AI Act.

Another innovative aspect of the article is the introduction of a novel approach to the study of the SPS implementations in various settings. This paper is informative, and the alternative approaches would be analyzed in-depth as a way of finding the middle ground between legal legitimacy and technical advancement. This, coupled with the fairness-by-design model where monitoring and responsibility are transparent and enforceable, has proved to be necessary towards growing inclination to trust in police work and long-term acceptance of enlisting the support of smart techniques of policing.

Notably, practical and policy-oriented recommendations to the stakeholders that can be given are the value addition to the study. The findings suggest the ongoing monitoring of the indicators on fairness and accountability and self-governing structures of control and the introduction of the best practices worldwide into the local context. The other important issue that was brought up in the study is how the policymakers, technology developers and legal practitioners ensure that the SPS implementations are not contravening international norms and social expectations. This is what can give the future developments of the changes that will take the necessities of the future into consideration of the emerging issues on privacy of data, algorithmic discrimination, and reliance on vendors. Finally, this article provides a new criterion of how operational excellence can be achieved with high rates of legal security, which strengthens the idea of SPS as an effective and valid concept in the digitalization of the criminal justice system.

8.2 Recommendations

In order to ensure a healthy and responsible use of the Smart Police Stations (SPS), governments need to establish independent watchdog bodies that will often audit the practices of the AI-based policing treatment to ensure that there is transparency and accountability. These legislations should be modified to incorporate some elements to safeguard privacy and data rights, extend conceptual consent and visibly show opt-out guidelines against automated decision-making. In order to establish trusting relationships on the establishment level, the stakeholder outreach operations, such as the social conversations and technological collaboration between law enforcement agencies, technology producers and the civil society, need to be systematized such that the SPS realizations are aligned with the local value and social problem domains. The technical crews need to embrace fairness-by-design methods like constant bias testing and reasonable AI modutor to identify and alleviate discriminatory outcomes in real time. Finally, cross-sectoral training development should be developed in such a way that the law enforcement officers, law professionals and system operators possess advanced experience in digital liberties and data security, and the SPS systems should be ethically operated long-term.

8.3 Study Limitations

Some severe shortcomings exist in this research. Preceding research is mainly based on secondhand data and published material, and there is the probability that this may not cover the depth of the picture regarding the stakeholder perceptions or the emerging issues during the implementation that go hand in hand with the Smart Police Stations (SPS). Second, differences between various regions (and, in particular, between Gulf and European contexts) complicate the comparisons made between various areas, because such differences may be seen in the form of differences in the data usage, the stage of the regulatory maturity, and the very access to the important institutional records, and this variation may precondition the existence of the possibility to transfer findings across the jurisdictions. Third, there is no longitudinal empirical evidence on the development of the popular trust, confirmation of the fairness criteria, and the live efficiency of the operation of the SPS systems, which predisposes the fact that it is difficult to assess the long-term sustainability and dynamic force of the SPS systems, and why future field research and open participation of stakeholders is a necessity.

8.4 Study Implications and Future Directions

Findings of the current study give some insights that could be utilized by the practitioners and policy makers in an attempt to host and operate Smart Police Stations (SPS) more expeditiously. The encouragement of methodological nature and the transparency of the approach lead to the evolution of the value of fairness-by-design, the observable nature, and the legislation of digital policing. Institutional training, a set of regulatory rules, and models of the cross-sector partnership might build such results and could support a balance of the technological innovations, customer trust, and legal protection. The longitudinal and mixed-method research would be preferable to take up in future works to address the measurement of fairness, transparency, and trust; the research should examine the empirical results of independent oversight systems, consent management processes, and stakeholder engagement procedures under various sociocultural conditions.

Funding

This research was conducted solely by the author and did not receive funding from any governmental, private, or non-profit entities.

Conflict of Interest

The author declares no conflicts of interest that could have influenced the study or its outcomes.

Acknowledgments

This research was funded by Naïf Arab University for Security

Sciences under grant No. NAUSS-25-R19

References

[1] Ma A. Regulation in pursuit of artificial intelligence (AI) sovereignty: China's mix of restrictive and facilitative modalities. The African Journal of Information and Communication (AJIC). 2024;34:1-16. Doi: https://doi.org/10.23962/ajic.i34.20103

[2] Alvarez JM, Colmenarejo AB, & Elobaid A. Policy advice and best practices on bias and fairness in AI. Ethics & Information Technology. 2024;26:31. Doi: https://doi.org/10.1007/s10676-024-09746-w

[3] Alsharif K, & Tarhini A. Predictive policing and algorithmic fairness: Rethinking risk, responsibility and regulation. Synthese. 2023;201(206). Doi: https://doi.org/10.1007/s11229-023-04189-0

[4] Bokhari SAA, Park SY, & Manzoor S. Digital government transformation through artificial intelligence: The mediating role of stakeholder trust and participation. Digital. 2025;5(3):43. Doi: https://doi.org/10.3390/digital5030043

[5] Cheong BC, Goh CL, & Chong K. Transparency and accountability in AI systems: Safeguarding well-being in the age of algorithmic decision-making. Frontiers in Human Dynamics. 2024;6. Doi: https://doi.org/10.3389/fhumd.2024.1421273

[6] Lahusen C, Maggetti M, & Slavkovik M. Trust, trustworthiness and AI governance. Scientific Reports. 2024;14:20752. Doi: https://doi.org/10.1038/s41598-024-71761-0

[7] Novelli C, Arigoni E, & Sartor G. Accountability in artificial intelligence: What it is and how it works. AI & Society. 2024;39(3):1201–1220. Doi: https://doi.org/10.1007/s00146-023-01635-y

[8] Hicken CA. A comparative analysis of the factors influencing the efficacy of police performance in the Dubai Police Force, United Arab Emirates, as against Nigeria Police Force, Nigeria, with lessons for the Guyana Police Force. Journal of Human Resource and Sustainability Studies. 2024;12:456-485. Doi: https://doi.org/10.4236/jhrss.2024.123026

[9] Sachoulidou A. Going beyond the "common suspects": To be presumed innocent in the era of algorithms, big data and artificial intelligence. Artificial Intelligence and Law. 2023;31(4):789–840. Doi: https://doi.org/10.1007/s10506-023-09347-w

[10] Muñoz JE. Psychophysiological insights and user perspectives: enhancing police de-escalation skills through full-body VR training. Frontiers in Psychology. 2024;15. Doi: https://doi.org/10.3389/fpsyg.2024.1390677

[11] An S, Cheung CF, & Willoughby KW. A gamification approach for enhancing older adults' technology adoption and knowledge transfer. Technological Forecasting and Social Change. 2024;205:123456. Doi: https://doi.org/10.1016/j.techfore.2024.123456

[12] Karlsson K, & Dalipi F. Exploring the surveillance technology discourse: A bibliometric analysis and topic-modeling approach. Frontiers in Artificial Intelligence. 2024;7. Doi: https://doi.org/10.3389/frai.2024.1406361

[13] Springs D. Smart city planning focused on the US cities in need of policing innovations and public health safety technologies and strategies. Health Economics and Management Review. 2024;5(1):117-128. Doi: https://doi.org/10.61093/hem.2024.1-09

[14] Al-Saidi M, & Zaidan E. Smart cities and communities in the GCC region: from top-down city development to more local approaches. Frontiers in Built Environment. 2024;10. Doi: https://doi.org/10.3389/fbuil.2024.1341694

[15] Rawindaran N, Nawaf L, Alarifi S, Alghazzawi D, Carroll F, Katib I, & Hewage C. Enhancing cyber-security governance and policy for SMEs in Industry 5.0. Digital. 2023;3(3):200-231. Doi: https://doi.org/10.3390/digital3030014

[16] Hung TW, & Yen CP. Predictive policing and algorithmic fairness. Synthese. 2023;201(6). Doi: https://doi.org/10.1007/s11229-023-04189-0

[17] Almasoud AS, & Idowu JA. Algorithmic fairness in predictive policing: A systematic review and mitigation of age-related bias. AI and Ethics. 2024;5(3):2323-2337. Doi: https://doi.org/10.1007/s43681-024-00541-3

[18] Han Y, Cai J, Ma E, Du S, & Lin J. Understanding Smart City Practice in Urban China: A Governance Perspective. Sustainability. 2023;15(9):7034. Doi: https://doi.org/10.3390/su15097034

[19] Gstrein OJ. General-purpose AI regulation and the EU AI Act. Internet Policy Review. 2024;13(1). Doi: https://doi.org/10.14763/2024.3.1790

[20] Alshaleel MK. The extraterritoriality of the GDPR and its effect on GCC businesses. Global Journal of Comparative Law. 2024;13(2):201–226. Doi: https://doi.org/10.1163/2211906X-13020004

[21] Finocchiaro G. The regulation of artificial intelligence. AI & Society. 2024;39:1961-1968. Doi: https://doi.org/10.1007/s00146-023-01650-z

[22] Gültekin-Várkonyi G. Navigating data governance risks: Facial recognition in law enforcement under EU legislation. Internet Policy Review. 2024;13(3). Doi: https://doi.org/10.14763/2024.3.1798

[23] Gyevnar B, Ferguson N, & Schafer B. Bridging the transparency gap: What can explainable AI learn from the EU AI Act? Frontiers in Artificial Intelligence and Applications. 2023;372:964-971. Doi: https://doi.org/10.3233/FAIA230367

[24] Lynch N. Facial recognition technology in policing and security—Case studies in regulation. Laws. 2024;13(3):35. Doi: https://doi.org/10.3390/laws13030035

[25] Qandeel M. Facial recognition technology: Regulations, rights and the rule of law. Frontiers in Big Data. 2024;7. Doi: https://doi.org/10.3389/fdata.2024.1354659

[26] Fabri M. From court automation to e-Justice and beyond in Europe. International Journal for Court Administration. 2024;15(1):1-9. Doi: https://doi.org/10.36745/ijca.640

[27] Ferrara E. Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. Sci. 2023;6(1):3. Doi: https://doi.org/10.3390/sci6010003

[28] Cevallos ID, Benalcázar ME, Valdivieso Caraguay ÁL, Zea JA, & Barona-López LI. A systematic literature review of machine unlearning techniques in neural networks. Computers. 2025;14(4):150. Doi: https://doi.org/10.3390/computers14040150

[29] Sarzaeim P, Mahmoud QH, Azim A, Bauer G, & Bowles I. A systematic review of using machine learning and natural language processing in smart policing. Computers. 2023;12(12):255. Doi: https://doi.org/10.3390/computers12120255