P-ISSN 2664-0422	Pakistan Social Sciences Review	July-September 2025, Vol. 9, No.3
O-ISSN 2664-0430	https://doi.org/10.35484/pssr.2025(9-III)28	[338-350]

Pakistan Social Sciences Review
www.pssr.org.pk

RESEARCH PAPER

AI-Driven Policing in Pakistan: Potential Pitfalls, and Privacy Concerns

[1]Saeed Ahmed Soomro*, [2]Hadi Bakhsh Kalhoro, and [3]Mahwish Gujjar

1. Post Graduate Scholar, Department of Criminology, University of Sindh, Jamshoro, Sindh, Pakistan
2. PhD Scholar, Department of Criminology, University of Sindh, Jamshoro, Sindh, Pakistan.
3. LLM Scholar, Institute of Law, University of Sindh, Jamshoro, Sindh, Pakistan.

***Corresponding Author:** soomrosaeedahmed40@gmail.com

ABSTRACT

This study aims to assess the perceived and actual benefits of AI-driven policing and to examine the legal, ethical, and operational challenges in Pakistan, focusing specifically on urban centers. AI technologies such as facial recognition, predictive analytics, and automated surveillance are being increasingly deployed in Pakistani law enforcement. However, this technological expansion has occurred in the absence of robust regulatory frameworks and public accountability mechanisms, raising concerns about civil liberties and democratic oversight. This is a qualitative secondary research study based on thematic analysis of academic literature, official reports, legal documents, and civil society publications. The findings indicate uneven implementation across cities, a lack of algorithmic transparency, and significant institutional capacity deficits. While AI offers improvements in surveillance and crime detection, its unregulated use poses risks to privacy and social equity. The study calls for a national legal framework, independent oversight bodies, and inclusive governance to ensure ethical and rights-based AI policing.

KEYWORDS Artificial Intelligence (AI), Smart Policing, Predictive Policing, Privacy Rights, Algorithmic Bias, Data Protection, Law Enforcement, Digital Governance, AI Ethics

Introduction

Digital technologies are already radically changing the landscape of law enforcement, especially Artificial Intelligence (AI). Police institutions across the globe are starting to implement AI technology to transform the classic methods of policing in favor of more foreseeable, actively reactive, and surveillance-driven approaches to community security. This is not simply a technological change, but a rearrangement of the terms of the state and its subjects, a transformation of how criminality is pre-empted, how suspects are found, and how justice is achieved (Ferguson, 2019; Joh, 2017). Artificial Intelligence in its different applications in face recognition, machine learning, video analytics, natural language processing, and predictive modeling, has emerged as the cornerstone of an activity that scholars refer to as smart policing (Brayne, 2017). With complex algorithms, real-time analysis of huge datasets, identification of behavioral patterns, recognition of faces and license plates, even flagging suspicious activities is possible using AI systems. Such capabilities will contribute to safer crime prevention, minimizing human mistakes, and maximizing the law enforcement budget in ever more complicated urban areas (Garvie, Bedoya, & Frankle, 2016).

Policing that is AI-based has already been institutionalized in different measures in countries such as the United States, China, and the United Kingdom. The example is China or its so-called Skynet project that connects to more than 600 million surveillance

cameras featuring facial recognition technology to track the movement of people (Mozur, 2018). Police departments in the U.S. have been implementing predictive algorithms to predict crime hotspots and thus better patrol them, and in the UK, an experiment was conducted over live facial recognition in the event of a demonstration. Yet, with the emergence of such technological advancements, there have been valid concerns of algorithm bias, racial profiling, and privacy invasion, as well as that of transparency and accountability (Buolamwini & Gebru, 2018; Eubanks, 2018). In the case of Pakistan, a state that faces a complex set of security issues, including terrorism and sectarian violence as well as crime in urban areas and insurgency, there is a sentiment among many policymakers that the use of AI in policing models is not only desirable but also unavoidable. In major cities, including Lahore, Islamabad, Karachi, etc., the chronic problems are the police departments are not well equipped with the resources, criminal databases are outdated and responses are slow and there is no formula of inter agency coordination. Such drawbacks are even worsened by population pressure, political instability, and increasing demands of the populations to become secure and efficient (International Crisis Group, 2016). Over the past decade, Pakistan has taken tangible steps toward integrating AI and digital technologies into its policing infrastructure. One of the most prominent examples is the Punjab Safe Cities Authority (PSCA), established in 2015 through collaboration between the Punjab government and Huawei Technologies. The PSCA's flagship project in Lahore has deployed over 8,000 high-definition surveillance cameras across the city, linked to a centralized control room equipped with AI-powered facial recognition and vehicle tracking systems (PSCA, 2018). These systems not only monitor real-time activity but also assist in criminal investigations, traffic management, and emergency response coordination. Similarly, the Islamabad Safe City Project**,** launched with assistance from Chinese firms, employs an integrated command and control center connected to thousands of cameras, automated number plate recognition (ANPR), and GPS-enabled patrol vehicles (Dawn, 2020). Though less developed, Karachi has initiated pilot projects involving AI-assisted mobile surveillance vans, biometric identification systems, and proposals for crime mapping based on digital footprints (Express Tribune, 2022).

These initiatives suggest a growing consensus among Pakistani authorities that AI can address critical weaknesses in law enforcement capacity. There is optimism that with the help of automation and real-time data analytics, police forces can become more proactive, responsive, and efficient—especially in high-crime areas and during mass public events. The ability to track suspects, prevent organized crime, and streamline evidence management has been lauded by security experts as a "force multiplier" for underperforming police departments (Ali & Nisar, 2021). However, this optimism must be tempered by caution. Despite the visible deployment of AI tools in some Pakistani cities, the legal and institutional frameworks governing these technologies remain either underdeveloped or entirely absent. Unlike the European Union's General Data Protection Regulation (GDPR), Pakistan has no comprehensive data protection law. The Prevention of Electronic Crimes Act (PECA) 2016—the country's primary cyber law—offers only vague provisions on surveillance, lacking explicit guidelines on biometric data, algorithmic accountability, or oversight of AI-driven tools used by public authorities (Shah, 2020; DRF, 2021).

Furthermore, there is a high possibility of abuse in politically divided communities such as Pakistan. Civil liberties groups (including the Digital Rights Foundation and Media Matters for Democracy) have also been repeatedly issuing warnings that the adoption of facial recognition technologies and mass surveillance systems may be applied to silence any form of dissent or persecute all those who may

oppose the above-considered technologies (DRF, 2021). The uncertainty with regard to algorithmic decision-making and the inability to completely communicate with the masses add more weight to the concerns of the surveillance state. The international investigations have also found out that most AI systems possess inherent biases which are usually informed by biased training data. The results of a seminal study published by Buolamwini and Gebru (2018) showed that facial recognition algorithms used by various companies, have much higher error rates by darker-skinned women than lighter-skinned men, which increases the presence of doubts about its use in racially and ethnically heterogeneous societies. Although Pakistan has not carried out any mass audits of its AI mechanisms, there is no denying the threat of racial profiling and the false identification of individuals, especially in a place where sectarian discrimination has been the norm and political oppression is still possible.

Literature Review

Within the past decade, the scholarly debate regarding the subject of AI-aided policing has expanded considerably, concentrating on its effect on policing efficacy, societal domination, citizen confidence, and legal vicinity. The use of algorithmic systems to redefine the use of state power has been a point of study among scholars particularly in societies where security issues are a major concern. This literature review explores key thematic strands relevant to the Pakistani context, namely: (1) the governance of algorithmic decision-making; (2) the sociopolitical impacts of surveillance technologies; (3) the global digital divide in AI infrastructure; (4) human rights critiques of biometric and AI systems; (5) Institutional Readiness and Capacity Deficits; and (6) Comparative Perspectives on Regulatory and Legal Safeguards.

Algorithmic Governance and The Logic of Automation

Algorithmic policing systems operate within what Ziewitz (2016) calls a new "logic of automation," wherein decisions are increasingly offloaded to machine-based systems with limited human oversight. Scholars such as Kitchin (2014) and Pasquale (2015) have warned that opaque algorithmic operations reduce the space for democratic scrutiny and may normalize surveillance as a default mode of governance. These concerns become more pronounced in contexts where rule of law is weak or selectively applied—as is often the case in developing countries. In the absence of algorithmic accountability, the risk of error or bias becomes embedded in the system itself. For instance, O'Neil (2016) argues that many predictive policing models are "weapons of math destruction" because they rely on historical crime data that may reflect existing institutional biases, such as over-policing of low-income communities. The problem is not only technical but deeply political: data-driven policing can reinforce discriminatory patterns under the guise of objectivity, particularly when algorithmic outputs are treated as infallible (Eubanks, 2018). In Pakistan, where there is no formal AI ethics body or algorithmic audit mechanism, such concerns take on added urgency. The unchecked reliance on proprietary or foreign-developed systems—without public debate, legal clarity, or operational transparency—raises fundamental questions about who is accountable when AI systems make mistakes or produce discriminatory outcomes.

Surveillance Technologies And The State-Citizen Relationship

Another important line of literature connects the growth in the use of AI-based technologies to monitor people to other changes in the relationship between the state and its subjects. Information societies and flows According to Lyon, information flows allow

surveillance societies to sort, classify and control populations, often creating patterns that correspond to social hierarchies (Lyon, 2007). The issue of postcolonial states, such as, Pakistan, where colonial practices of hierarchical control continue in policing institutions, is that the new surveillance infrastructures could bolster authoritarian governance under the rhetoric of modernization (Singh, 2020). Besides, Monahan (2009) and Andrejevic (2007) observe that surveillance technologies have the potential of creating an atmosphere of mistrust, especially within the open areas and lead to distrust between the communities and the police. This is particularly applicable to the multiethnic urban centres of the country already affected by ethnic, sectarian and linguistic minority stigmatization and state overstretch in Pakistan. This may also alienate these groups since they are not consulted on the deployment of surveillance, or asked to contribute. The results of empirical research on the concept of smart policing in other Southeast Asian countries and those of the Global South (India and Brazil) indicate that such policing operations frequently result in more search and corresponding scrutiny of vulnerable populations instead of crimes prevention (Kumar, 2021; Diniz, 2020). This evidence serves as a warning to the idea of techno-solutions and the need to consider the social and political background when looking at the effects AI may have on people on a wider scale concerning the topic of public safety.

The Global Digital Divide in AI Infrastructure

The current literature on structural asymmetries between the Global North and South in accessibility to AI, its design, and application has a significant literature base. As countries in the developed world are paving the AI future path by investing huge sums of money in research and in developing their own algorithm, most developing nations are bound to imported technologies, many of which they have little control over their operation, not to mention the data traffic (Taylor & Broeders, 2015). This reliance may lead to the so-called digital subordination, in which countries have no option to create their own AI-related tools or to audit foreign code, as Graham and Dutton (2014) state. The majority of facial recognition, surveillance, and data analysis platforms in Pakistan are outsourced or installed bilaterally with the Chinese firms, either Huawei (Raza, 2019). This brings the issue of digital sovereignty, cyber security and geopolitical power into play. According to scholars, the absence of local development capabilities would mean Pakistan turning into a passive consumer of black box technologies. Furthermore, in the absence of sound regulatory frameworks, such technologies can be exploited to support civil liberties as opposed to supporting the rule of law (Ahmed, 2021). The literature therefore suggests establishing local AI talent, creating national legal traditions-based ethical frameworks, and building native capacity.

Biometric Data, Privacy, and Human Rights

Finally, a growing literature from human rights and legal scholars critiques the proliferation of biometric surveillance, including facial recognition, iris scans, and gait analysis. According to Breckenridge (2014), the global biometric turn marks a shift from universal citizenship rights to systems of identity verification based on bodily data. While these systems can improve service delivery or national security, they also centralize control over identity and erode the anonymity that underpins freedom of movement and expression. Privacy scholars like Solove (2006) argue that surveillance harms are often misunderstood: the danger lies not only in exposure, but in aggregation, classification, and misuse. Biometric data, once compromised, cannot be reset like passwords. In countries without data protection laws—like Pakistan—this creates a serious vulnerability. There have already been reports of leaked national ID data from

Pakistan's National Database and Registration Authority (NADRA), raising concerns about how facial recognition and video analytics tools are being integrated with existing national databases (Digital Rights Foundation, 2021). Moreover, international human rights law—including Article 17 of the International Covenant on Civil and Political Rights (ICCPR)—recognizes the right to privacy as a fundamental liberty. The UN Special Rapporteur on the Right to Privacy has repeatedly called for moratoriums on facial recognition until robust legal safeguards are in place (UNHRC, 2020). Pakistan, as a signatory to ICCPR, has an international obligation to ensure that emerging policing technologies do not infringe on privacy, freedom of expression, or the presumption of innocence.

Institutional Readiness and Capacity Deficits

Another significant strand in the literature focuses on institutional readiness for AI deployment in policing. According to Heeks (2018), the success of AI in public sector innovation is contingent not only on technology, but on bureaucratic culture, inter-agency collaboration, and legal maturity. In low-resource states, institutions often adopt technologies faster than they can regulate or understand them—a phenomenon termed technological leapfrogging without governance anchoring. Scholars such as Ada Lovelace Institute (2021) stress the importance of data stewardship—the ability of public institutions to collect, store, share, and protect sensitive data responsibly. Pakistan's institutional frameworks for data stewardship are weak and fragmented. National databases such as NADRA or Safe City Project repositories operate in silos, with little to no interoperability or independent oversight (Rizvi, 2021). Moreover, the absence of impact assessments, ethics committees, or judicial warrant requirements in surveillance rollouts makes accountability virtually impossible. The literature also emphasizes the challenge of human capital. AI systems require trained personnel to program, monitor, and interpret machine-generated outputs. Pakistan's police forces—often overburdened and under-trained—lack dedicated digital forensics units or algorithmic audit teams (Khan & Abbas, 2022). Without capacity-building, AI tools may be poorly implemented, misinterpreted, or abandoned altogether.

Comparative Perspectives on Regulatory and Legal Safeguards

A comparative review of global AI-policing frameworks reveals that Pakistan lags significantly behind in regulatory oversight. Countries like Canada and the Netherlands have begun introducing AI-specific ethical charters, mandating human-in-the-loop decision-making, regular audits, and community review boards (Cavoukian, 2013; Government of Netherlands, 2020). In contrast, Pakistan's PECA 2016 contains no references to AI, predictive analytics, biometric data use in policing, or digital due process. The EU Artificial Intelligence Act (2021), though not yet finalized, proposes a risk-based classification of AI systems. Applications in law enforcement are categorized as "high-risk," requiring strict transparency, documentation, and human oversight. Such models could be instructive for Pakistan's policymakers. Similarly, the UK Biometrics and Surveillance Camera Commissioner provides independent reviews of police use of facial recognition and makes reports accessible to the public—mechanisms absent in Pakistan. Scholars such as Mantelero (2018) propose the principle of "data protection by design and by default", where surveillance systems must embed privacy safeguards from the inception. In Pakistan, data-intensive technologies are often adopted without privacy impact assessments or community feedback. For example, the deployment of Safe City projects in Lahore and Islamabad occurred under executive orders without parliamentary debate or civil society involvement (Shah, 2020). This top-down approach

not only undermines transparency but may violate constitutional protections under Article 14, which guarantees the privacy of the home and dignity of citizens.

Material and Methods

This study adopts a qualitative, exploratory research design based on secondary data analysis to examine the implementation of AI-driven policing in Pakistan. Given the limited availability of primary data on algorithmic policing in the country, this approach allows for a comprehensive synthesis of academic literature, policy documents, legal texts, and civil society reports. The research is based on a descriptive and interpretive research design, which appeals to the manner in which AI technologies (e.g., facial recognition, predictive analytics, and surveillance) are operationalized in Pakistan, and implications of such technologies on rights, accountability, and governance. The sources include peer-reviewed journals, organizations reports such as Punjab Safe Cities Authority (PSCA) and the NADRA, publications such as the Digital Rights Foundation (DRF) and the Human Rights Commission of Pakistan (HRCP). International legal regulations, including the EU Artificial Intelligence Act and the UNHRC privacy reports, were examined as well to give them relatively context.

Thematic content review was used to conduct the analysis and determine the recurring patterns that included algorithmic bias, institutional capacity, and overreach of surveillance. Although the study does not focus on a direct production of the primary data, like interviews or field observation, however, the study gives a comprehensive picture of cross-verification of various and credible sources. Ethical Standards were adopted via open sourcing references, and fairness of opinions. Although enforcement of data access and state transparency is limited, the study will provide valuable insight on trends and dangers of AI policing in Pakistan.

Results and Discussion

The integration of Artificial Intelligence (AI) into policing frameworks in Pakistan reveals a multi-layered and uneven evolution, one marked by a complex interplay of technological promise, institutional inertia, regulatory voids, and democratic vulnerabilities. Drawing from official project documentation, civil society analyses, comparative international frameworks, and scholarly evaluations, this section discusses key findings across the three research objectives. While AI technologies offer practical solutions to long-standing policing deficiencies—such as understaffing, delayed response times, and poor crime mapping—these innovations, in the Pakistani context, are marred by a lack of oversight, equity, and clarity of purpose.

Perceived and Actual Benefits of AI in Law Enforcement

In the discourse of law enforcement modernization, AI-driven policing is often portrayed as a strategic solution to Pakistan's resource-constrained and overburdened police forces. The rhetoric surrounding Safe City projects, particularly in Lahore under the Punjab Safe Cities Authority (PSCA), reflects a broader state narrative that links AI implementation to better crime control, operational precision, and proactive governance. AI tools like facial recognition technology (FRT), automated number plate recognition (ANPR), real-time surveillance, and automated crime detection systems are increasingly framed as critical "force multipliers" (PSCA, 2019). Indeed, in Lahore, over 8,000 high-definition cameras are connected to a centralized command and control center, supported by facial recognition and analytics software. The PSCA reports increased

capacity to identify and track criminal suspects, recover stolen vehicles, monitor traffic violations, and coordinate emergency responses through AI-powered alert systems. Similar efficiencies are reported from the Islamabad Safe City Project, where AI-supported surveillance aids in situational awareness and management of high-risk zones (Dawn, 2020).

However, outside of institutional discourses, there exists no empirical (or peer-reviewed) analysis supporting any long-term crime-deterring effects or meaningful transformations in police accountability. Though temporary strategic advantage can possibly be noticed (increased traffic surveillance or a speedy apprehension), the overall effect on crime patterns, community confidence, and justice provision is questionable. Furthermore, the success of AI technology is commonly mixed with pre-existing surveillance or policing potential, so it may be hard to understand the pure effects of AI measures. Moreover, the use of AI in policing in Pakistan enables the blind exploration of criminality causes, including socioeconomic deprivation, a lack of access to justice, and weak rule of law. According to researchers, such as Eubanks (2018) as well as Ferguson (2019), AI might institutionalize operational policing but cannot resolve systematic problems such as police abuse, corruption, and community unlegitimacy, an issue that is particularly acute in Pakistan where the police frequently proceed without any oversight by civilians and have been charged with extrajudicial means. In this context, AI is in danger of becoming a folksy fix which patches over rather than fixes deep institutional problems.

Uneven Implementation of AI across Urban Centers

One of the clearest findings of this study is that the deployment of AI-powered policing technologies in Pakistan is highly centralized, fragmented, and politically uneven. Lahore stands as the most technologically advanced city in terms of AI policing infrastructure, largely due to sustained provincial political support, external partnerships (particularly with Chinese firm Huawei), and significant public investment under the PSCA. This initiative has resulted in an expansive surveillance network, real-time data dashboards, and AI-based analytics for crowd control, traffic management, and criminal tracking. In Islamabad, the capital's Safe City Project initially launched with similar ambitions but has suffered from reported inefficiencies, hardware failures, cost escalations, and misalignment between federal and local police authorities. Technical evaluations have revealed underperformance in maintenance and system responsiveness due to a lack of trained personnel and inter-agency communication (Express Tribune, 2022).

Karachi, Pakistan's largest metropolis, presents a much more challenging picture. Despite being a hub for crime and militancy in recent decades, Karachi has not benefited from coordinated AI policing infrastructure. The city suffers from institutional fragmentation, with overlapping jurisdictions between city police, Sindh Rangers, and federal intelligence agencies. Efforts at deploying AI tools remain limited to isolated interventions—such as mobile surveillance vans, manual facial recognition via mobile apps, or camera installations in commercial zones—without integration into a centralized database or analytics platform. This creates a patchwork of capabilities with inconsistent standards and minimal effectiveness.

More importantly, AI policing initiatives continue to be entirely inaccessible to smaller cities and rural communities. Lack of one national policy or framework on the digital policing has resulted in the geographic and governance imbalances, with access

to modern tools of surveillance depending on the local political orientations and donor relations. It is a town oriented strategy which places a risk of two tier security i.e. the areas where only elite areas are placed with technological improvements and the areas that are not well policed or covers high-risk areas have to either be neglected or applied traditional method which most of the time is coercive only. Moreover, the excessive use of external technology suppliers and especially Chinese vendors casts a doubt about data localization, compatibility of the systems, and sustainability. The lack of bilateral agreements or technical capacity in these provinces prevents them to independently work in the field of AI policing, increasing technological dependence and contributing to reinforcing regional disparities.

Technological, Legal, and Ethical Challenges

The operationalization of AI in the Pakistani policing process shows little structural success beyond high-profile deployments due to deeply rooted obstacles impacting the efficacy of the technologies and the democratic passage. In the technological sector, Pakistan does not have local capabilities in terms of the development of AI models, the validation of algorithms, and assurances of cyber security. Safe City surveillance platforms and most other surveillance platforms are constructed as black-box systems to which neither the police nor oversight institutions are provided access or insight into the software code, reasoning, or training data. Such a lack of transparency, further in combination with the lack of independent auditing, however, increases the likelihood of technical issues, false positives, and algorithmic bias, which already have been reported in the international setting, including the United States and United Kingdom (Buolamwini & Gebru, 2018). Devoid of the capability to question or rectify such biases, there compose a serious risk that the AI policing systems in Pakistan will disproportionally persecute minority groups that were previously oppressed (i.e. religious minorities, ethnic minorities, and political dissidents).

Pakistan is in a regulatory abyss as far as the legal front is concerned. Despite being the most referred cyber law, the Prevention of Electronic Crimes Act (PECA) 2016 lacks any specifications regarding AI, biometric data regulation, or facial recognition policies. No Data Protection Authority has ever been established, and draft legislation languishes in a parliamentary cul-de-sac after years. Consequently, no formal requirements are made to obtain informed consent, or warrants by the judicial authorities to surveil, and data minimization requirements. This regulatory gap creates the opportunity of mission creep, meaning that the tools AI applies in the name of public safety can find a quieter application in political surveillance and protest monitoring, or profiling because of ideas and beliefs other people hold and hope to escape legal change. Civil society groups like Digital Rights Foundation (2021) and Human Rights Commission of Pakistan (2021) have expressed their concern over the potential usage of facial recognition to target people at political rallies, university, religious events with little or no transparency or safeguarding procedures in place.

Ethically, ethical questions encapsulate the idea of the expansion of AI surveillance and its implications of matters relating to the state-citizen status, informational autonomy, and even the right of anonymity in the open world. The use of undesirable surveillance mechanisms undermines the freedom of assembly, expression and privacy convection guaranteed by the Constitution of Pakistan and South Asia obligations including the International Covenant on Civil and Political Rights (ICCPR). Making these issues even worse is the fact that people are not educated on AI systems. The majority of citizens do not know the location of surveillance cameras, with its

purpose being utilized via facial recognition and still have not been educated regarding their rights as a human under digital surveillance systems. This leads to dis-empowerment of the masses not to mention the fact that it interferes with democratic norms of openness and accountability. AI policing in Pakistan is likely to be even more of a control mechanism without public deliberation, consent mechanisms, and civic education on the tool of justice.

Conclusion

The field of law enforcement in Pakistan is undergoing a massive transmutation by Artificial Intelligence because it is providing opportunities to enhance the surveillance, detection, and the prevention of crimes in new forms. However, as the given research shows, the institutional and legal preparedness of the country to adopt such transformational technology is weak. The example of the Punjab Safe Cities Authority shows that AI can be used to improve security and emergency operations in cities, but the fact that there is no regulatory framework, control processes, and transparency guidelines sounds alarm bells. AI policing has been implemented largely without legal guidelines, without debate, or external oversight, and thus there is much potential to abuse AI policing at the risk of the state overreaching its ability resulting in misuse in already a highly politically polarized society with a track record of excess power by the state.

The disproportionate availability of AI infrastructure in selected metropolitan regions is one more threat of widening the regional security and governance gap. In addition, the dependence on overseas suppliers, in particular, on Chinese technology suppliers, questions the sovereignty of data and the financial independence of the country in the long term. In the end, the future of AI-based policing in Pakistan depends not only on technological potential but, above all, on the ethical and democratic guidelines of where and how such technologies are used. There is an urgent need to shift towards the human rights-based model of AI governance that involves transparency and citizen trust in Pakistan. This will involve the enactment of data protection laws, establishment of autonomous regulating agencies, sensitizing the civil society in monitoring, and indigenous technological capabilities. In absence of such actions, the potential of AI policing will proceed into a surveillance state that risks deteriorating the basic rights of the citizens in Pakistan as opposed to safeguarding them.

Recommendations

Artificial Intelligence in policing presents both practical advantages in terms of efficiency and serious implications to privacy, civil liberties, democratic governance, and institutional integrity. In Pakistan, where the legislative and oversight ecosystem is not sufficiently developed, the blistering application of AI tools should be supplemented with sound policy interventions. The proposed measures will encourage an accountable, lawful, and open AI-based law enforcement procedure.

- Enact a comprehensive national legal framework specifically regulating the use of AI in law enforcement, with clear definitions, scope, and limitations aligned with constitutional protections and international human rights standards.

- Establish an independent Data Protection Authority empowered to oversee biometric data collection, algorithmic decision-making and AI-based surveillance practices, including mechanisms for redress and public complaints.

- Mandate algorithmic transparency and accountability in all AI systems used by police, including regular third-party audits, impact assessments, and publication of performance metrics to ensure fairness, accuracy, and non-discrimination.

- Introduce binding requirements for human oversight ("human-in-the-loop") in all AI-supported policing decisions, particularly those related to facial recognition, predictive analytics, and automated criminal profiling.

- Ban the use of facial recognition and real-time surveillance technologies in sensitive contexts such as political protests, religious gatherings, and university campuses, until adequate safeguards and judicial warrant protocols are in place.

- Encourage the development of indigenous AI solutions through public-private partnerships and academic research, reducing dependence on foreign vendors and strengthening digital sovereignty.

References

Ada Lovelace Institute. (2021). *AI and the public interest: Principles for governance*. Ada Lovelace Institute. https://www.adalovelaceinstitute.org

Ahmed, A. (2021). AI governance and digital sovereignty in Pakistan: A policy gap analysis. *Journal of South Asian Policy Studies*, *6*(1), 24–39.

Ali, S., & Nisar, M. (2021). Public safety and the rise of surveillance technologies in Pakistan. *Pakistan Journal of Criminology*, *13*(1), 15–34.

Amnesty International. (2020). *Human rights in Asia: Pakistan chapter*. https://www.amnesty.org

Andrejevic, M. (2007). *iSpy: Surveillance and Power in the Interactive Era*. University Press of Kansas.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. *ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review, 82*(5), 977–1008.

Breckenridge, K. (2014). *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge University Press.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, *81*, 1–15.

Cavoukian, A. (2013). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca

Dawn. (2020, January 14). Safe City Project: Achievements and shortfalls. *Dawn News*. https://www.dawn.com

Digital Rights Foundation (2021). Biometric surveillance in Pakistan: A human rights perspective. *Digital Rights Foundation*. https://digitalrightsfoundation.pk

Diniz, G. (2020). Smart Surveillance in Brazil: Technologies of Control and Resistance. *Latin American Research Review, 55*(3), 462–479.

Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.

Express Tribune. (2022, May 4). Karachi Safe City project facing delays and setbacks. *The Express Tribune*. https://tribune.com.pk

Feldstein, S. (2019). *The Global Expansion of AI Surveillance*. Carnegie Endowment for International Peace. https://carnegieendowment.org

Ferguson, A. G. (2019). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

Garvie, C., Bedoya, A., & Frankle, J. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Georgetown Law Center on Privacy & Technology.

Government of Netherlands. (2020). *Framework for the Responsible Use of Algorithms in Government*. Ministry of the Interior and Kingdom Relations. https://www.government.nl

Graham, M., & Dutton, W. (2014). *Society and the Internet: How Networks of Information and Communication are Changing Our Lives*. Oxford University Press.

Green, B. (2021). *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. MIT Press.

Heeks, R. (2018). *Information and Communication Technology for Development (ICT4D)*. Routledge.

Human Rights Commission of Pakistan. (2021). *State of human rights in 2020*. HRCP. https://hrcp-web.org

International Covenant on Civil and Political Rights. (1966). United Nations General Assembly. UN. https://www.ohchr.org/en/instrumentsmechanisms/instruments/international-covenant-civil-and-political-rights

International Crisis Group. (2016). *Reforming Pakistan's Criminal Justice System*. Asia Report No. 196. https://www.crisisgroup.org

Joh, E. E. (2017). Artificial Intelligence and Policing: First Questions. *Seattle University Law Review, 41*(2), 425–444.

Khan, M., & Abbas, R. (2022). AI and Police Modernization in Pakistan: Opportunities and Institutional Challenges. *Lahore Journal of Governance, 3*(2), 44–58.

Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*. Sage.

Kumar, A. (2021). Surveillance and Caste in Indian Policing: A Critical Perspective. *Surveillance & Society, 19*(2), 149–165.

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity Press.

Mantelero, A. (2018). *AI* and Data Protection: Challenges and Recommendations. *Computer Law & Security Review, 34*(4), 674–682.

Meijer, A., & Wessels, M. (2019). Predictive Policing: Review of Benefits and Drawbacks. *International Journal of Public Administration, 42*(12), 1031–1039.

Monahan, T. (2009). Surveillance and Inequality. *Surveillance & Society, 5*(3), 283–286.

Mozur, P. (2018, July 8). Inside China's Dystopian Dreams: AI, Shame and Lots of Cameras. *The New York Times*.

O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown Publishing.

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press.

Punjab Safe Cities Authority. (2018). *Annual report*. Government of Punjab. https://psca.gop.pk

Punjab Safe Cities Authority. (2019). *Annual performance report 2018–2019*. Government of Punjab. https://psca.gop.pk

Raza, M. (2019). *Safe* Cities and Chinese Tech: Data Colonialism in Pakistan? *South Asia Cybersecurity Brief, 3*(1), 12–18.

Rizvi, N. (2021). Pakistan's Data Governance Deficit: A Case Study of NADRA and the Safe City Project. *Policy Perspectives, 18*(1), 62–81.

Shah, B. (2020). PECA and the Problem of Digital Surveillance in Pakistan. *Media Matters for Democracy.*

Siddiqa, A. (2007). *Military Inc.: Inside Pakistan's Military Economy*. Pluto Press.

Singh, A. (2020). Postcolonial Policing and Surveillance Infrastructures in South Asia. *International Journal of Comparative Criminology, 8*(1), 55–78.

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477–564.

Taylor, L., & Broeders, D. (2015). In the Name of Development: Power, Profit and the Datafication of the Global South. *Geoforum, 64*, 229–237.

Tyler, T. R. (2004). Enhancing Police Legitimacy. *The Annals of the American Academy of Political and Social Science, 593*(1), 84–99.

United Nations Human Rights Council. (2020). *Report of the Special Rapporteur on the Right to Privacy*. https://www.ohchr.org

Ziewitz, M. (2016). Governing Algorithms: Myth, Mess, and Methods. *Science, Technology, & Human Values, 41*(1), 3–16.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.