

Algorithmic Transparency in Judicial Decision-Making:

Safe City Surveillance, FRT, ANPR, NADRA Biometric Integration, the Black Box Problem, and the Constitutional Right to a Fair Trial

*Mian Umer Arshad*¹

ABSTRACT

Authorities across all four provinces has established an algorithmic law enforcement apparatus of unprecedented scale. This integrated triad, comprising Facial Recognition Technology (FRT), Automatic Number Plate Recognition (ANPR), and NADRA-integrated biometric databases, currently operates in a near-complete legal vacuum. This article employs a doctrinal-analytical methodology to demonstrate that the deployment of such opaque algorithmic evidence constitutes a tripartite constitutional violation of Article 9 (Life and Liberty), Article 10-A (Fair Trial), and Article 14 (Dignity and Privacy).

The central thesis posits that the constitutional standard of a meaningful defence is structurally impossible when evidence is generated by "Black Box" systems whose internal logic remains inaccessible to the accused, counsel, and the court. By drawing upon a comparative analysis of landmark Pakistani and international judicial precedents, and documenting systemic harms such as wrongful arrests and erroneous automated citations, the research identifies a critical Transparency Deficit. The study concludes by proposing a robust five-tier legislative reform framework. This includes suggested amendments to the Qanun-e-Shahadat Order 1984 and the Investigation for Fair Trial Act 2013, the enactment of a statutory Right to Explanation, and the establishment of a National Algorithmic Evidence Commission to ensure that technological utility does not supersede constitutional sanctity.

¹ Advocate High Court, Independent Legal Researcher, Sialkot, Pakistan.

The author can be reached at: umerap11@gmail.com

Keywords: *Algorithmic Transparency; FRT; ANPR; NADRA Biometric Integration; Article 10-A; Fair Trial; Meaningful Defence; Black Box; Explainability Crisis; Algorithmic Evidence Disclosure Standard; Artificial Intelligence; Rebuttable Presumption; Safe City Pakistan; QSO Article 59; QSO Article 164; Bridges v CCSWP; Puttaswamy; EU AI Act 2024*

Introduction

Pakistan's Safe City infrastructure operates two distinct categories of autonomous decision-making that together constitute the most significant unregulated use of AI against citizens in the country's legal history. The first Facial Recognition Technology (FRT) generates probabilistic criminal identifications that can trigger arrests. The second Automatic Number Plate Recognition (ANPR) automatically issues financial penalties to vehicle owners, with a documented error rate that has produced thousands of wrongful challans across Pakistan. Both categories share a fundamental constitutional defect: neither requires, as a condition of its legal effect, any disclosure of the system's accuracy, methodology, or the probability of error in the specific case. Both produce outcomes arrest, charge, penalty before the affected citizen has any mechanism to challenge the algorithmic decision. And both rely on the same black box opacity that renders meaningful challenge structurally impossible.

When a Safe City facial recognition algorithm matches a face captured on a camera in Lahore with a criminal database entry, the effect will be the arrest, remand, or framing of charge consequently leading to the trial. All this would happen without ensuring the accuracy of the system and without giving such information to an accused, the arresting officer, the prosecutor, or the presiding judge. There is also a lack of information of how confident the match was, or how often systems of this type misidentify people of the accused's demographic characteristics. This is not a hypothetical scenario. In October 2025, Karachi police publicly announced the first arrest in Sindh province made primarily on the basis of Safe City facial recognition data.² No Technical Disclosure Statement was filed with the court. No probability score was disclosed to the defence. No independent audit had ever been conducted of the Sindh Safe City FRT system's accuracy, on

Pakistan's ethnically and phenotypically diverse population. The accused was produced before a Judicial Magistrate. The algorithm had spoken. No human being present in that courtroom could explain why.

Pakistan's Safe City infrastructure has grown at a pace that has comprehensively outrun its legal framework. The Punjab Safe Cities Authority (PSCA)², established under the Punjab Safe Cities Authority Act 2016 (Act I of 2016)³ in collaboration with Huawei Technologies, operates over 8,000 high-definition cameras installed in Lahore. This has also expanded to Faisalabad, Rawalpindi, Gujranwala, and eighteen additional districts linked to an AI-powered Integrated Command, Control and Communication (IC3) system with real-time FRT and Automatic Number Plate Recognition (ANPR) capabilities. The Islamabad Safe City project monitors the capital with integrated FRT, ANPR, and GPS coordination. The Sindh Safe Cities Authority, whose legislation was amended on 13 January 2026,⁴ operates 42 FRT units among Karachi's 900-plus camera network. KPK maintains its own Safe City framework for Peshawar⁵. And in February 2026, the Balochistan Cabinet approved the Balochistan Safe City Project⁶, completing Pakistan's national AI-powered surveillance footprint. These are not passive recording systems. They actively classify, identify, and generate alerts and ANPR-generated penalties that affect citizens' liberty, mobility, and finances every day.

This article employs a doctrinal-analytical methodology, systematic textual examination of constitutional provisions, statutory

² Punjab Safe Cities Authority, "Official Portal", PSCA, <https://psca.gop.pk/> (accessed March 14, 2026).

³ The Punjab Safe Cities Authority Act 2016 (Act XVI of 2016), Government of the Punjab, available at: https://punjablaws.punjab.gov.pk/uploads/articles/PUNJAB_SAFE_CITIES_AUTHORITY_ACT_2016.pdf (accessed March 14, 2026).

⁴ The Sindh Safe Cities Authority Act 2026 (Sindh Act No. II of 2026), Provincial Assembly of Sindh, available at: https://pas.gov.pk/uploads/acts/Sindh_Act_No.II_of_2026.pdf (accessed March 14, 2026).

⁵ Government of Khyber Pakhtunkhwa, "Project Management Unit (PMU) for Peshawar Safe City Project", KP Official Portal, <https://kp.gov.pk/page/pmuforpeshawarsafecityproject> (accessed March 14, 2026).

⁶ Balochistan Safe Cities Authority, "Official Portal", BSCA, <https://bsca.gob.pk/> (accessed March 14, 2026).

instruments, and judicial precedent, supplemented by comparative constitutional analysis and empirical case studies from Pakistan and internationally.

Core Research Question

Does algorithmic opacity in Safe City FRT, ANPR, and NADRA-integrated biometric evidence violate Article 10-A of the Constitution of Pakistan 1973 and what specific legal reforms are constitutionally required in response?

Algorithmic Justice: Conceptual Framework and Pakistani Context

The concept of 'algorithmic justice' has emerged as the primary normative framework for evaluating AI systems deployed in public decision-making. As articulated by Qureshi, Ahmed, and Chaudhary (2025), algorithmic justice encompasses four interlocking requirements: transparency (the ability to understand how an AI reaches its decisions); non-discrimination (freedom from bias based on race, gender, ethnicity, or class); due process (the right to know and challenge the basis of algorithmic decisions); and accountability (clarity about who bears responsibility when algorithms cause harm).⁷ Pakistan's Safe City AI systems, as this article demonstrates, fall short of all four requirements.

The significance of algorithmic justice is amplified by Pakistan's unique legal pluralism, which combines Islamic jurisprudence, British colonial common law, and customary norms. The principle of عدل (justice) in Islamic jurisprudence demands that no person be condemned on evidence they cannot comprehend or challenge. The

⁷ G. M. Qureshi, F. A. Ahmed, & F. Chaudhary, "Algorithmic Justice and Legal Pluralism", *Competitive Research Journal Archive*, Vol. 3, No. 2 (2025), pp. 67–75, available at: <https://thecrja.com/index.php/Journal/article/view/106> (accessed March 14, 2026). **Note:** For the original and authoritative text of the statutes mentioned in this article, please refer to the Official Gazette of Pakistan or <https://pakistancode.gov.pk>

common law adversarial tradition, inherited through Pakistan's Code of Criminal Procedure 1898⁸ and the Qanun-e-Shahadat Order 1984⁹, makes cross-examination of evidence central to the trial, additionally, in civil matters, the principles of the Civil Procedure Code 1908¹⁰ ensure that procedural fairness remains a cornerstone for adjudicating evidence in algorithmic contexts. The principle of *ijtihad* (independent legal reasoning) supports the conclusion that traditional procedural guarantees must be reinterpreted for the AI context and that algorithmic transparency is not merely a technical preference but a constitutional and jurisprudential necessity.

Pakistan's AI Governance Gap

Pakistan's governance architecture for AI and emerging technologies remains fragmented and normatively narrow. The National AI Policy (Draft, 2023)¹¹ introduced by the Ministry of IT is overwhelmingly techno-centric, focused on productivity and innovation, with minimal engagement with justice, fairness, or algorithmic accountability. There is no judicial discourse on algorithmic bias, no procedural framework for evaluating algorithmic evidence, and no parliamentary debate on the constitutional implications of AI-powered law enforcement. As Soomro, Kalhoro, and Gujjar (2025) document, Pakistan's AI-driven policing infrastructure has been built in the absence of robust regulatory frameworks and public accountability

⁸ *The Code of Criminal Procedure, 1898*, available at: <https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Npa5lp-sg-iiiiiijiiiiii> (Accessed: June 20, 2026).

⁹ Qanun-e-Shahadat Order, 1984, Art. 164, available at: <https://pakistancode.gov.pk/english/UIY2FqaJw1-apaUY2Fqa-apaUY2Npa5plaw%3D%3D-sg-jijijijijijiji> (Accessed: June 20, 2026).

¹⁰ *The Code of Civil Procedure, 1908*, available at: <https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apeb-sg-ijiiiiiiiiii> (Accessed: June 20, 2026)

¹¹ Ministry of Information Technology & Telecommunication, "*National AI Policy Consultation Draft V1*", Government of Pakistan (2023), available at: <https://moitt.gov.pk/Siteline/Misc/files/National%20AI%20Policy%20Consultation%20Draft%20V1.pdf> (accessed March 14, 2026).

mechanisms.¹² The algorithms that identify faces, read number plates, and flag suspicious behaviour were developed abroad, trained on foreign datasets, and operate with no public disclosure about accuracy rates, percentage of error margins, or demographic performance. This is what Frank Pasquale (2015) terms the 'black box society' a world in which consequential decisions are made by opaque algorithms that citizens and courts cannot interrogate.¹³

What is Black Box

The term 'black box,' originating in systems theory, denotes any system whose inputs and outputs are observable but whose internal processing is opaque neither reducible to human-comprehensible logical rules nor expressible in a chain of reasoning that can be examined.

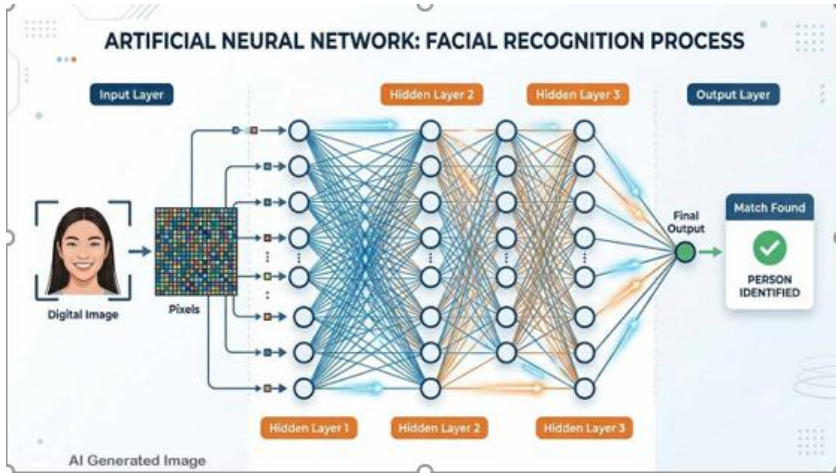
1. Facial Recognition Technology (FRT): Operation, Problems, and Case Law

1.1 How FRT Works: The Black Box and the Explainability Crisis

Pakistan's Safe City FRT systems employ deep learning “Neural Networks/ ***A neural network is a computational model that processes data through interconnected layers of nodes to identify patterns and generate outputs based on learned relationships***) computational architectures trained on large datasets of labelled face images.

¹² S. A. Soomro, H. B. Kalhor, & M. Gujjar, "AI-driven policing in Pakistan", Pakistan Social Sciences Review, Vol. 9, No. 3 (2025), pp. 338–350, available at: <https://ojs.pssr.org.pk/journal/article/view/1065> (accessed March 14, 2026).

¹³ Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press (2015), available at: <https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf> (accessed March 14, 2026).



During training, millions of numerical parameters are adjusted to optimise the network's ability to match input face images to database entries. When a camera captures an image, the trained network transforms it into a probability vector and outputs a match if the highest probability score exceeds the configured threshold. The critical legal point is that this computational process contains no logical rules, no explicit criteria, and no human-comprehensible account of why a particular image was matched to a particular person. The neural network does not reason. It computes. This is what AI scholars term the 'Explainability Crisis' the fundamental structural impossibility of producing, for any specific output of a deep neural network, a causal explanation in human-intelligible terms.¹⁴

The critical legal point is that this process contains no logical rules, no explicit criteria, and no human-comprehensible account of why a particular image was matched to a particular database entry. The neural network does not 'see' a face the way a human witness sees it. It does not identify a nose, or eyes, or a distinctive scar. It processes pixel arrays through mathematical transformations of such complexity that the system's own developers, after the fact cannot reconstruct, in any judicially meaningful sense, why the network assigned a match

¹⁴ F. Doshi-Velez & B. Kim, "Towards a Rigorous Science of Interpretable Machine Learning", arXiv preprint arXiv:1702.08608 (2017), available at: <https://arxiv.org/pdf/1702.08608> (accessed March 14, 2026).

score of 0.89 to person A and not to person B. This is what AI scholars term the Explainability Crisis the fundamental impossibility, for deep learning systems at the current state of the art, of producing a human-comprehensible explanation of any specific decision.¹⁵

The Explainability Crisis is not a temporary engineering problem. It is intrinsic to the deep learning paradigm: the statistical optimisation that makes these systems highly accurate on average is precisely the process that makes individual decisions inexplicable. Even the system's developer, given an input image and a match output, cannot reconstruct a chain of reasoning because there is no chain of reasoning, only a mathematical transformation through millions of numerical weights. From legal view it is always required before the court of law for giving a verdict and for the exercise of state power against individuals, indeed this is a constitutional problem of the first magnitude.

1.2 FRT: Documented Problems and Pakistani Cases

Investigative reporting on Pakistan's Safe City surveillance systems highlights the involvement of international technology vendors in the deployment of large-scale CCTV and monitoring infrastructure. In the case of Lahore's Safe City project, concerns were raised regarding the presence of foreign-supplied hardware components within surveillance systems, prompting discussions about security, oversight, and potential misuse of embedded technologies.¹⁶ Existing literature on facial recognition systems highlights the importance of performance evaluation across diverse demographic groups. In Pakistan's context, publicly available information regarding the assessment of such systems across different population groups

¹⁵ G. Shah, Z. Ali, & M. Tahir, "AI Integration in Pakistan's Legal System", Federal Law Journal, Vol. 4, No. 1 (2025), pp. 87–101, available at: https://flj.gov.pk/docs/v4_issue_1/v4_issue_1_art5.pdf (accessed March 14, 2026).

¹⁶ BBC News, "Algorithmic bias: The computer programs that learn to be racist," March 28, 2017, <https://www.bbc.com/news/technology-47856098> (Accessed: June 19, 2026).

remains limited.¹⁷ The MIT Media Lab study by Joy Buolamwini and Timnit Gebru (2018)¹⁸ established error rate disparities of up to 34.7% across demographic groups in leading commercial FRT systems, with the highest error rates concentrated among darker-skinned individuals.

The October 2025 Karachi FRT Arrest:¹⁹ Media reports concerning an October 2025 arrest in Karachi suggest that facial recognition technology was used as part of the investigative process in identifying a proclaimed offender. However, publicly available reporting provides limited information regarding the evidentiary role of the algorithmic output in subsequent judicial proceedings. Consequently, the case is more appropriately viewed as an illustration of the emerging use of FRT in law enforcement rather than as a definitive legal precedent concerning the admissibility or reliability of algorithmic evidence.

In *Nasira Ashfaq v. Director General, Safe Cities Authority* (W.P. No. 78006/2023)²⁰, the Lahore High Court dealt with issues arising from a request for access to surveillance-related material within the Safe City framework. The dispute primarily concerned the availability and disclosure of digital records, including CCTV footage, in the context of criminal investigation and the right of the accused to access potentially relevant material. While the case was not directly focused on facial recognition technology, it nonetheless brought into focus broader questions regarding the management, preservation, and accessibility of surveillance data held by public authorities. The proceedings reflect the increasing intersection between digital surveillance systems and

¹⁷ Digital Rights Foundation, *Annual Report 2023*, available at: <https://digitalrightsfoundation.pk/wp-content/uploads/2024/04/DRF-Annual-Report-2023.pdf> (Accessed: June 20, 2026).

¹⁸ Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", *Proceedings of Machine Learning Research*, Vol. 81 (2018), pp. 1–15, available at: <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (accessed March 14, 2026).

¹⁹ Imtiaz Ali, "Suspect arrested in Karachi with help of facial recognition technology", *Dawn*, Oct 21, 2025, <https://www.dawn.com/news/1950258> (accessed March 14, 2026).

²⁰ *Nasira Ashfaq v. Director General, Safe Cities Authority*, 2025 PCrLJ 233 (Lahore High Court)

procedural safeguards in criminal justice, particularly in relation to transparency and fair trial considerations.

1.3 FRT and the Article 59 QSO Expert Evidence Problem

The Punjab Safe Cities Authority Act 2016 (PSCAA), Section 14(2), read with Article 59 of the Qanun-e-Shahadat Order 1984 and Section 510 of the Code of Criminal Procedure 1898, provides for the use of PSCA information technology personnel as evidentiary witnesses in proceedings involving digital systems and related technological outputs. Article 59 QSO governs the admissibility of expert opinion evidence in matters requiring specialised knowledge, while its evidentiary value is determined by the court under established principles relating to admissibility, qualification, methodology, and cross-examination. Section 14(2) of PSCAA 2016 operates as a deeming provision for evidentiary purposes under Article 59 QSO. The assessment of whether a witness is suitable to provide such opinion evidence is carried out by the court under the general framework governing expert evidence, having specialised knowledge with relevance, and evidentiary value. The statutory provisions do not set out detailed procedural requirements regarding the manner in which technical testimony is linked to the digital systems forming the basis of evidentiary outputs, thus leaving such assessment to the general evidentiary framework applicable under the QSO.

In the context of AI-based facial recognition systems, questions have been raised regarding the extent to which such testimony can fully capture algorithmic decision-making processes, particularly where system complexity and proprietary constraints limit detailed disclosure of underlying models. This creates an emerging tension between traditional expert evidence standards and the technical realities of AI-enabled surveillance.

The evolution of electronic evidence in Pakistan reflects a gradual shift from basic recognition of digital records to more structured treatment of system-generated data. The Electronic Transactions Ordinance 2002 introduced legal recognition of electronic documents, while the Prevention of Electronic Crimes Act 2016 further developed the framework by defining information systems and addressing digital evidence in criminal investigations.

This development largely assumes a system-reliability approach focused on data integrity. However, the rise of AI-based tools such as facial recognition adds new challenges, particularly in relation to fair trial guarantees under Article 10-A²¹ of the Constitution. In *Dr. Mobashir Hassan and others v. Federation of Pakistan and others*²² the Supreme Court emphasised the constitutional importance of the right to a fair trial under Article 10-A, particularly in ensuring that criminal proceedings remain subject to meaningful procedural safeguards and judicial scrutiny of evidence. The judgment underscores the broader principle that evidentiary processes must allow adequate opportunity for challenge within the framework of due process.

2. Automatic Number Plate Recognition (ANPR): Operation, Problems, and Case Law

2.1 How ANPR Works and Its Distinct Legal Character

ANPR systems use optical character recognition neural networks to read number plates from camera images, matching results against vehicle and excise databases to identify violations, wanted vehicles, or to generate e-challans for traffic offences. Like FRT, ANPR operates through a deep learning pipeline, the neural network performs character segmentation and recognition through millions of learned parameters that produce no human-comprehensible account of why a specific character was read as a '3' rather than an '8', or a 'B' rather than an '8'. ANPR is subject to the same Explainability Crisis as FRT but presents a distinct and in some respects more immediate constitutional problem, because ANPR systems generate legal obligations directly and automatically, without any human intermediary between the algorithmic output and the financial penalty.

The operational reliability of ANPR systems may be affected by adverse environmental conditions that degrade image quality

²¹ Article 10-A, The Constitution of the Islamic Republic of Pakistan, 1973 (Inserted via the Constitution (Eighteenth Amendment) Act, 2010, guaranteeing the fundamental right to a fair trial and due process).

²² *Dr. Mobashir Hassan v. Federation of Pakistan* (Suo Motu Case No. 13 of 2010 regarding the National Reconciliation Ordinance), PLD 2012 SC 649.

and reduce detection and recognition accuracy. Studies published in MDPI (Axioms, 2023, 12(5):424)²³ on automated number plate recognition indicate that adverse weather conditions such as fog, haze, and rain can degrade image quality and, in certain circumstances, reduce detection and recognition accuracy.

Reported cases of erroneous e-challans in Pakistan²⁴ underscore the risk of misidentification in automated number plate recognition systems. This issue is worsened by cloned or tampered plates, where the system's inability to distinguish between identical strings from different provincial series effectively reverses the burden of proof. By issuing automated penalties without accuracy disclosure, these systems bypass the Article 10-A mandate of 'fair trial' and undermine the constitutional presumption of innocence.

The constitutional framework for challenging administrative action Article 199²⁵ writ jurisdiction, and the principle in *Government of Sindh v. Shaikh Salahuddin*²⁶ that administrative action affecting fundamental rights requires clear statutory authority applies in full. Yet no mechanism currently provides a citizen with the algorithmic basis of the ANPR identification before the penalty takes effect. The constitutional framework governing administrative action remains applicable to technology-assisted enforcement measures. While established criminal jurisprudence places the initial burden on the prosecution or enforcing authority to prove its case, emerging forms of digital evidence raise new questions regarding reliability and scrutiny. Comparative jurisprudence, most notably the *Daubert* standard,²⁷ emphasises judicial assessment of scientific reliability, including

²³ Axioms 12, no. 5 (2023): 424, <https://www.mdpi.com/2075-1680/12/5/424> (Accessed: June 21, 2026).

²⁴ Customer Surprised After Receiving Rs. 10,000 Wrong E-Challan," *PakWheels Blog*, (October 25, 2023), <https://www.pakwheels.com/blog/ur/customer-surprised-after-receiving-rs-10000-wrong-e-challan/> (Accessed: June 19, 2026).

²⁵ Article 199, The Constitution of the Islamic Republic of Pakistan, 1973 (Jurisdiction of High Court to enforce fundamental rights and review administrative actions).

²⁶ *Government of Sindh v. Shaikh Salahuddin*, PLD 1992 Supreme Court 463, Supreme Court of Pakistan.

²⁷ *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993); see also *Cornell Law School, Legal Information Institute, "Daubert Standard,"* available at: https://www.law.cornell.edu/wex/daubert_standard (Accessed: June 19, 2026).

testing, error rates, and methodological validity. Similar concerns can be seen in Pakistani case law. In *Muhammad Ammar Shafi v. The State*,²⁸ the Lahore High Court declined to place reliance on CCTV and PSCA-generated material where foundational requirements relating to authentication, expert verification, forensic examination, and chain of custody had not been satisfied. The decision suggests that technology-generated outputs are not exempt from evidentiary scrutiny. As Pakistani courts have yet to articulate specific standards for AI-driven identifications, the evidentiary treatment of algorithmic outputs remains an evolving area of law.

2.2 ANPR: Documented Problems and Pakistani Cases

Systematic ANPR Wrongful Challans: Throughout 2024, 2025, and 2026, thousands of vehicle owners across Punjab, Sindh, and Islamabad received incorrect ANPR-generated e-challans arising from camera misreads (especially of similar-looking alphanumeric characters), cloned or duplicated plates, camera angle and lighting failures, and Excise Department database mismatches.²⁹ The PSCA e-challan system provides mechanisms for users to contest or review issued challans, including an online review option available through the online system as well as official communication channels such as helpline and email support for rectification of disputed entries, where discrepancies may be addressed through established verification procedures.³⁰ No legislation requires ANPR systems to meet any minimum accuracy threshold before deployment. No pre-issuance human review is mandated. The citizen bears the entire burden of proving the error after the penalty has been issued and has begun to affect their ability to use or transfer their vehicle.

Munir Ahmad v. Government of Punjab (2024):³¹ The matter is pending before the Honorable Lahore High Court, and guidelines regarding the validity of ANPR e-challan are anticipated on its

²⁸ *Ammar Shafi v. The State*, 2025 YLR 1681, Lahore High Court.

²⁹ PSCA E-Challans Pakistan, <https://e-challans.pk/how-to-remove-a-wrong-e-challan-in-pakistan/> (Accessed: June 19, 2026)

³⁰ PSCA Launches E-Challan Complaint System, " <https://www.techjuice.pk/psca-e-challan-complaint-system-launch/>; Punjab Safe Cities Authority, "How to Review E-Challan" (Official Video Tutorial), <https://www.youtube.com/watch?v=IWovIjbzmn8> (Accessed: June 19, 2026).

³¹ *Munir Ahmad v. Province of Punjab through Secretary Transport & Others*, W.P. No. 10174/2024, Lahore High Court (filed Feb 15, 2024) [Pending final adjudication].

adjudication. The petitioner challenged the constitutional validity of the ANPR e-challan system on the grounds that challans were being issued automatically by an algorithmic system without any human verification, without disclosure of the algorithmic basis for the identification, and without any pre-issuance mechanism for challenge. The court's engagement with this petition raised fundamental questions about whether the ANPR system's automated penalty generation without prior human review and without disclosure of the system's accuracy meets the 'in accordance with law' standard of Article 9 and the fundamental fairness requirement of Article 10-A as applied to civil penalties. The petition specifically questioned whether ANPR algorithmic evidence meets the 'reliability of mechanical process' standard under Article 164 QSO. These pertinent questions indicate a precise constitutional gap, in respect of which this study propose the insertion/amendment in Article 164 of QSO accordingly, as discussed later in this article.

In **Tariq Basra v. State**³² it was held that *"The prosecution cannot invite the court to act upon scientific evidence unless it has affirmatively established, through competent expert testimony, the reliability of the scientific process by which that evidence was produced. Any doubt about the accuracy or reliability of a scientific method must be resolved in favour of the accused. The burden of proof of reliability lies with the prosecution throughout."*

If the mandate given in *Tariq Basra* case is observed as a standard in ANPR matters, it is noted that it directs the authority and not to the citizens to affirmatively demonstrate ANPR accuracy before a challan can be enforced. In contrast the current system inverts this burden entirely by e- challans take effect automatically without any scrutiny, and the citizens are required to identify the error to defend themselves. Further, in view of the reliability standard explained in the above case, the current ANPR mechanism seems completely inconsistent and makes the presumption of innocence as is implicit in Article 10-A untenable while also limiting the rights of citizens of fair hearing and due process.

³² *Tariq Basra v. The State*, 2012 SCMR 1060, Supreme Court of Pakistan

2.3 ANPR and the Article 164 QSO Inadequacy

Article 164 QSO permits evidence produced by 'mechanical or other process' if the court is satisfied of the 'reliability of the mechanical process.' Drafted in 1984 for mechanical recording devices, this provision asks whether the device accurately captured what occurred a question about fidelity of recording. ANPR asks an entirely different question: did the neural network correctly classify which alphanumeric characters appear on this plate? A camera either recorded a scene faithfully or it did not. An ANPR system's character recognition involves probabilistic pattern matching through learned parameters, with error rates that vary by character similarity, plate condition, camera angle, weather, and lighting. Article 164 QSO provides no framework for this inquiry. It does not require disclosure of ANPR accuracy rates, does not address demographic or situational performance variations, and provides no mechanism for a citizen to challenge the algorithmic reading of their own number plate.

3. NADRA³³ Biometric Integration: Function Creep, Constitutional Violation, and Comparative Law

3.1 NADRA's Biometric Database: Scale and Constitutional Character

The National Database and Registration Authority (NADRA) maintains what is arguably Pakistan's most sensitive and consequential dataset. Over 98.3% of Pakistani citizens hold a Computerised National Identity Card (CNIC)³⁴, each issued after collection of fingerprints, facial photographs, iris scans, and signature. NADRA's database therefore constitutes a near-complete national biometric register of Pakistan's entire adult population a dataset of extraordinary sensitivity and constitutional significance, collected under the NADRA Ordinance 2000

³³ National Database and Registration Authority (NADRA), Official Portal, Government of Pakistan, available at: <https://www.nadra.gov.pk/> (accessed March 14, 2026).

³⁴ NADRA Over 98.3% of Pakistani citizens hold a CNICs," *Business Recorder*, June 25, 2024, available at: <https://www.brecorder.com/news/40408522> (accessed March 14, 2026).

and the NADRA Act 2012³⁵ for the specific, constitutionally justified purpose of civil registration and citizen identification.

The constitutional character of this data is clear, its collection was justified by the legitimate aim of civil administration enabling citizens to prove identity, access services, and exercise rights. No parliamentary legislation specifically authorises the sharing or integration of NADRA biometric data, particularly citizens' facial photographs, with law enforcement facial recognition systems or Safe City FRT matching databases. The NADRA Ordinance 2000 and NADRA Act 2012 authorise data sharing for verification purposes of establishing identity but do not expressly authorise the use of NADRA photographs to train FRT algorithms or to populate the criminal identification databases against which Safe City cameras conduct real-time matching.

3.2 Function Creep as Constitutional Violation

Data protection scholars term the gradual expansion of a collected dataset's use beyond its original authorised purpose 'function creep.' In constitutional terms, function creep is not merely a regulatory violation, it is a constitutional one. The Supreme Court held in *Human Rights Cases*³⁶ that government databases containing sensitive personal information attract heightened constitutional protection and that the State bears the burden of demonstrating clear legal authority for any use of such information beyond its original purpose. The use of NADRA biometric data for real-time population surveillance goes far beyond civil registration, it serves a categorically different purpose that requires independent constitutional justification and specific parliamentary authorisation that currently does not exist.

In *Suo Motu Case*³⁷ the Supreme Court held that mass surveillance without legislative authorisation constitutes a prima facie violation of Article 14 of Constitution, which guarantees dignity and

³⁵ National Database and Registration Authority (NADRA), "Legal Frameworks", Government of Pakistan, available at: <https://www.nadra.gov.pk/legalFrameworks> (accessed March 14, 2026).

³⁶ *Human Rights Cases*, PLD 2014 Supreme Court 699, Supreme Court of Pakistan.

³⁷ *Suo Motu Case No. 14 of 2019 (In re: Use of Technology in Courts)*, PLD 2020 Supreme Court 1, Supreme Court of Pakistan.

privacy. In *Muhammad Rahmatullah v. The State*³⁸ the Lahore High Court held that the constitutional right to privacy takes precedence over other inconsistent provisions of domestic law. The 2024 NADRA data breach, in which biometric details of approximately 2.7 million citizens were illicitly extracted and exported reveals the extreme sensitivity of the data and the inadequate data protection mechanism within existing infrastructure on which Pakistan's algorithmic identification system relies.

3.3 Comparative Law: India's Puttaswamy Framework and the Aadhaar Analogy

Justice K.S. Puttaswamy (Retd.) v. Union of India:³⁹ The Indian Supreme Court's landmark judgment about the most comprehensive judicial treatment of biometric data privacy in South Asian constitutional law recognised privacy as a fundamental right under Articles 19⁴⁰ and 21⁴¹ of the Indian Constitution. The Court held unanimously that informational privacy, the right to control the collection, use, and disclosure of personal information is an intrinsic component of the constitutional right to life and personal liberty. Justice D.Y. Chandrachud, writing separately, articulated the principle with direct relevance to the NADRA context:

In *Justice K.S. Puttaswamy v. Union of India (Aadhaar)*⁴² the Supreme Court upheld India's biometric identification system for public benefit purposes while explicitly restricting its use for surveillance or law enforcement purposes for which independent constitutional authorisation had not been given. The Court struck down Aadhaar's use for private sector verification and limited its law enforcement use on the ground that civil registration data cannot constitutionally be repurposed for surveillance without specific

³⁸ *Muhammad Rahmatullah v. The State*, 2024 PCr.LJ 1, Lahore High Court

³⁹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, Supreme Court of India, available at: https://en.wikipedia.org/wiki/Puttaswamy_v._Union_of_India (accessed March 14, 2026).

⁴⁰ Article 19, The Constitution of India (Guaranteeing freedom of speech and expression and other fundamental freedoms).

⁴¹ Article 21, The Constitution of India (Protecting life and personal liberty, judicially interpreted to include the fundamental Right to Privacy).

⁴² *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1, Supreme Court of India, available at: <https://privacylibrary.ccgmlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors> (accessed March 14, 2026).

parliamentary authorisation. The Puttaswamy and Aadhaar framework directly supports the analysis of Article 14, Constitution of Pakistan.

Article 14 of Constitution, protects human dignity and privacy and to be interpreted, consistently with the Supreme Court's direction in Muhammad Rahmatullah and Suo Motu Case No. 14 of 2019, it directs that NADRA biometric data collection for civil registration of citizens cannot be repurposed for mass criminal surveillance without specific parliamentary authorisation. The absence of such authorisation makes the current NADRA-Safe City FRT integration an ongoing constitutional violation.

3.4 Investigation for Fair Trial Act (IFTA) 2013⁴³ and the Proportionality Inversion

The Investigation for Fair Trial Act 2013 requires a prior judicial authorisation from High Court for targeted surveillance of specific individuals. Telephone tapping, or a targeted interference with one's personal communications also requires a High Court warrant. Yet it is crucial to understand the real-time facial recognition identification of entire city's population by using the data collected by NADRA through automated biometric processing of hundreds of thousands of citizens requires no authorization from any authority. It is unfathomable that such intrusive mass surveillance has minimal oversight with no prior authorisation mechanism which would affect a large number of population on daily basis compare to a targeted individual surveillance. This proportionality inversion is constitutionally untenable: a framework that protects targeted surveillance subjects more rigorously than mass surveillance subjects do not claim consistency with Articles 9 and 14 of the Constitution.

⁴³ *The Investigation for Fair Trial Act, 2013* (Act No. I of 2013), National Counter Terrorism Authority (NACTA), available at: <https://nacta.gov.pk/wp-content/uploads/2017/09/INVESTIGATION-FOR-FAIR-TRIAL-ACT.2013.pdf> (accessed March 14, 2026).

4. The Constitutional Framework: Articles 9, 10-A, 14, and 25

4.1 Article 10-A: Meaningful Defence and the Right to Explanation

Article 10-A provides: *"For the determination of his civil rights and obligations or in any criminal charge against him a person shall be entitled to a fair trial and due process."*

In *District Bar Association Rawalpindi v. Federation of Pakistan*⁴⁴ the Supreme Court established that Article 10-A demands substantive, not merely procedural, fairness, the accused must be able to conduct a meaningful defence. In *Muhammad Nawaz Sharif v. State*⁴⁵ the Court held that due process requires the ability to meaningfully challenge the evidence. This applies to black box algorithmic evidence FRT, ANPR, and NADRA-integrated identification and observed that the constitutional standard is structurally unmet: the accused cannot comprehend, test, or challenge the basis of the identification.

This article advances the argument that Article 10-A gives a Right of fair trial and due process. Therefore, the same constitutional right is to be given to every citizen for algorithmic evidence to receive a comprehensible account of the basis on which any such identification was generated. This is the logical extension of the right to cross-examine to the AI context. Additionally, in *Mst. Razia Sultana v. State*⁴⁶ the Supreme Court held that evidence obtained through unconstitutional means is inadmissible establishing the constitutional foundation for a statutory exclusionary rule for algorithmic evidence obtained without required authorisation.

⁴⁴ *District Bar Association Rawalpindi v. Federation of Pakistan*, PLD 2015 Supreme Court 401, Supreme Court of Pakistan.

⁴⁵ *Muhammad Nawaz Sharif v. The State*, PLD 2018 Supreme Court 714, Supreme Court of Pakistan.

⁴⁶ *Mst. Razia Sultana v. The State*, PLD 2011 Supreme Court 1, Supreme Court of Pakistan.

4.2 The Rebuttable Presumption Approach to Algorithmic Evidence

This article proceeds on the concern that judicial engagement with digital and algorithmic evidence may, in practice, risk an implicit presumption of reliability, whereby computer-generated outputs are accepted without sufficiently demanding proof of underlying system integrity or methodological transparency.

The Horizon litigation in the United Kingdom illustrates the risks associated with excessive reliance on computer-generated outputs without adequate opportunities for independent verification. Following the quashing of convictions in *Hamilton v. Post Office Ltd*⁴⁷ and the enactment of the Post Office (Horizon System) Offences Act 2024,⁴⁸ the case has become a cautionary example of the consequences that may arise when the reliability of technological systems is insufficiently scrutinised.

In Pakistan, Article 164 of the Qanun-e-Shahadat Order 1984 facilitates the admission of evidence derived from modern devices and scientific techniques, but provides limited guidance on the assessment of complex algorithmic systems. This article therefore proposes the adoption of a rebuttable presumption approach for algorithmic evidence, under which the prosecution would bear the burden of demonstrating reliability through a Technical Disclosure Statement before such evidence is relied upon. This proposal is consistent with the reliability concerns identified by Tariq Basra, the forensic verification requirements discussed by Ishtiaq Ahmed Mirza, and the risk-based regulatory approach reflected in the EU AI Act 2024.

4.3 Article 9, Article 14, and Article 25⁴⁹

Article 9 of the Constitution mandates a standard for deprivation of life or liberty save 'in accordance with law'. In *Sh. Liaquat*

⁴⁷ *Hamilton & Others v. Post Office Limited*, [2021] EWCA Crim 577, Court of Appeal (Criminal Division), England and Wales, available at: <https://www.judiciary.uk/wp-content/uploads/2022/07/Hamilton-Others-v-Post-Office-judgment-230421.pdf> (accessed March 14, 2026).

⁴⁸ Post Office (Horizon System) Offences Act 2024 (c. 14), United Kingdom, available at: <https://www.legislation.gov.uk/ukpga/2024/14> (accessed March 14, 2026).

⁴⁹ Article 25, The Constitution of the Islamic Republic of Pakistan, 1973 (Establishing the principle of equality before law and non-discrimination).

Hussain v. Federation of Pakistan,⁵⁰ it was held by the Supreme Court that the authorising law meets substantive standards of fairness and non-arbitrariness. An arrest based on an FRT identification without meeting substantive standard of accuracy and fairness fails this standard. Likewise, the dignity and privacy as promised under Article 14, the violation of NADRA integrated data, as referred “function creep” is discussed in Part V above. Moreover, guarantee of non-discrimination given under Article 25 is engaged by the documented demographic accuracy disparity in commercial FRT systems. Without mandatory demographic disaggregation in accuracy reporting, the Article 25 prohibition on discrimination is unenforceable against an algorithm as systematic over-identification of particular ethnic communities cannot be detected, measured, or judicially remedied.

5. Statutory Framework and Comparative International Standards

5.1 Safe City Legislation: Systematic Deficiencies

The Punjab Safe Cities Authority Act 2016, the Sindh Safe Cities Authority (Amendment) Act 2025, the KPK Safe City framework, and the Islamabad Safe City operating without dedicated federal legislation share a common structural pattern: sweeping powers to deploy AI-powered surveillance, with no accuracy standards, no prior judicial authorisation requirement, no transparency obligation, no right of pre-issuance challenge for ANPR challans, no demographic testing requirement, and no compensation mechanism for algorithmic harm. The Section 14(2) 'deemed expert' provision, while providing a pathway for algorithmic evidence into criminal proceedings, does not substitute for the Technical Disclosure Statement. The Balochistan Safe City Project, approved in February 2026 without any of these requirements, represents the last opportunity to build algorithmic accountability into Pakistan's national surveillance architecture by design.

⁵⁰ *Sh. Liaquat Hussain v. Federation of Pakistan*, PLD 1999 Supreme Court 504, Supreme Court of Pakistan.

5.2 Prevention of Electronic Crime Act (PECA) 2016⁵¹ and the Autonomous Harm Gap

The Prevention of Electronic Crimes Act 2016 regulates the human conduct with information system, the dissemination of such information also requires human intention under it liability framework. Whereas, a Safe City FRT algorithm if misidentifies a citizen, or an ANPR system issues a wrongful challan, the provisions of PECA provision are not applicable because in Safe City algorithm or in ANPR system no person gains unauthorised access and no human criminally misuses the system. The harm arose from an autonomous probabilistic process operating within its designed parameters while producing a harmful output without any human intervention. Therefore, PECA 2016 is structurally incapable of imposing liability or even addressing the accountability of an automated body, which eventually creates a gap between the existing laws on Electronic Crimes and the autonomous algorithmic system currently operational in the country.

Comparative International Standards

Jurisdiction	Framework	FRT & ANPR Standard	Judicial Remark	Key Lesson for Pakistan
EU (AI Act 2024)	Unacceptable risk (banned), High-risk (strict regulation), Limited-risk (transparency obligations), and Minimal-risk (no regulation).	Mandatory pre-deployment conformity assessment; Art. 13 transparency obligation; Art. 14 human review before any decision; real-time biometric surveillance prohibited except	'High-risk AI systems shall be designed to ensure sufficient transparency to enable users to interpret the system's	Enact AEDS covering both FRT and ANPR; mandatory pre-deployment AIA; parliamentary authorisation required not executive protocols

⁵¹ *The Prevention of Electronic Crimes Act, 2016* (Act No. XL of 2016), National Assembly of Pakistan, available at: https://na.gov.pk/uploads/documents/1470910659_707.pdf (accessed March 14, 2026).

Jurisdiction	Framework	FRT & ANPR Standard	Judicial Remark	Key Lesson for Pakistan
		judicially authorised	output' Art. 13 ⁵²	
UK (Bridges 2020; Horizon 2024)	Bridges v CCSWP: FRT needs precise legal basis + equality assessment. Horizon Act 2024: reversed computer reliability presumption	No implicit reliability presumption; full technical disclosure required; independent corroboration mandatory; equality impact assessment for demographic bias	'The legal framework was not sufficiently clear to indicate with adequate certainty the extent of the discretion conferred on the police Haddon-Cave LJ	Develop a structured, rebuttable reliability framework for Article 164 QSO digital evidence, including clear assessment standards, non-discrimination safeguards, and defined statutory authority for each algorithmic system.
United States (Williams 2024; Loomis 2016)	Williams settlement: FRT requires corroboration. Loomis: trade secrets cannot defeat due a process	Corroboration by independent reliable evidence before FRT arrest; algorithm is not determinative alone; trade secret cannot prevent reliability disclosure in criminal proceedings	'The right to challenge evidence is incompatible with algorithmic opacity protected by intellectual property law' — Loomis	Codify corroboration requirement in CrPC; AEDS must override trade secret protection in criminal proceedings; private right of action for wrongful identification

⁵² European Union Artificial Intelligence Act, Article 13: Transparency and Provision of Information to Users, <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-13> (Accessed: June 19, 2026).

Jurisdiction	Framework	FRT & ANPR Standard	Judicial Remark	Key Lesson for Pakistan
India (Puttaswamy 2017; Aadhaar 2018)	Privacy = fundamental right (Arts. 19 & 21). Biometric data: highest level of protection. Aadhaar: civil registration data cannot be repurposed for surveillance	Each new use of biometric data requires fresh constitutional justification; biometric data collected for civil registration cannot be used for surveillance without independent parliamentary authorisation	'Privacy is the ultimate guarantee of dignity... informational privacy is an intrinsic component of the right to life' Chandrachud J, Puttaswamy	Arts. 9, 10-A & 14 jointly support same protection; NADRA data repurposing requires specific parliamentary authorisation — executive protocols are constitutionally insufficient
Pakistan (Current)	A reading of Article 164 QSO and Section 14(2) PSCA Act suggests that neither expressly addresses issues such as algorithmic transparency, auditability, or disclosure requirements for AI-generated evidence.	No standard FRT and ANPR outputs used without TDS, probability score, demographic accuracy data, or corroboration. ANPR challans issued with no pre-issuance human review	The Supreme Court's interpretation of Article 10-A underscores the importance of procedural fairness, including an effective opportunity to challenge evidence relied upon in legal proceedings. <i>Dr. Mobashir Hassan and others v. Federation of Pakistan and others</i> , PLD 2012 SC 649.	All five proposals in Part VIII are constitutionally required as a minimum standard requirement. Pakistan is currently below every comparable jurisdiction's standard

6. Reform Framework: Five Targeted Legal Proposals

The following five proposals address FRT, ANPR, and NADRA biometric integration. Each is grounded in the constitutional analysis of Part 4, the statutory analysis of Part 5, and the comparative foundations above.

1. New Article 164-A QSO: Algorithmic Evidence Disclosure Standard (AEDS)

The most urgent and constitutionally necessary reform is the insertion of a new Article 164-A in the Qanun-e-Shahadat Order 1984, establishing the Algorithmic Evidence Disclosure Standard as a mandatory pre-condition for the admissibility of any algorithmic identification evidence FRT, ANPR character recognition, or any other autonomous classification system in criminal or quasi-criminal proceedings. Article 164-A simultaneously introduces the Rebuttable Presumption standard, replacing the implicit infallibility presumption with an affirmative prosecution burden.

2. Statutory Right to Explanation (Article 10-A Implementation)

Parliament should enact a statutory Right to Explanation as the legislative implementation of Article 10-A in algorithmic contexts. Any person subject to arrest, charge, remand, conviction, or administrative penalty in which algorithmic evidence played a material role has a statutory right to receive, within 48 hours of written request, a plain-language written explanation of: the algorithm's role in the decision; the basis and confidence level of any identification or classification; and the system's known demographic error rates. This right is enforceable through Article 199 High Court writ jurisdiction mandamus compelling production; certiorari quashing proceedings founded on inadmissible algorithmic evidence. No trade secret protection shall be invoked to deny the Right to Explanation in criminal or quasi-criminal proceedings. Where the deploying authority cannot produce a compliant explanation, the algorithmic evidence shall be excluded.

3. Safe City Legislation: Mandatory Algorithmic Impact Assessment

A mandatory Algorithmic Impact Assessment (AIA) before any FRT or ANPR system is to be deployed or upgraded in Pakistan's Safe City legislation, including the Punjab PSCA Act 2016, the Sindh Safe Cities Authority Act, the KPK framework, and the forthcoming Balochistan enabling legislation. The AIA must document accuracy on a Pakistan-specific demographic validation dataset across major ethnic communities, false positive and negative rates disaggregated by gender, age, and ethnicity for ANPR, error rates by vehicle type, plate age, font format, camera placement, and lighting conditions; the identification threshold; human review requirements before any alert triggers police or administrative action; and the NADRA integration through a legal authorisation. Any system exhibiting a false positive rate for any demographic group more than twice the system-wide rate must be suspended. The Balochistan Safe City Project presents the final opportunity to build these requirements in their design.

4. IFTA 2013 Amendment, AI Criminal Evidence Act, and Legal Remedies

IFTA 2013 are to be amended to add Section 4-A requiring prior High Court authorisation for real-time FRT population scanning and NADRA biometric integration, with Section 26-A establishing a statutory exclusionary rule for evidence obtained without authorisation giving legislative expression to *Mst. Razia Sultana's constitutional principle*⁵³. Pakistan needs to enact a standalone Artificial Intelligence (Criminal Evidence) Act establishing a three-tier classification system for AI in criminal justice; mandatory NAEC registration for high-risk systems; annual accuracy and bias audits; a criminal offence of deploying unregistered AI in criminal proceedings; and a strict-liability civil right of action for persons wrongfully arrested or penalised by algorithmic error. Citizens have three immediate remedies: Article 199 writ; statutory civil action; and right to restrict data access/deletion under the forthcoming Personal Data Protection

⁵³ *Mst. Razia Sultana v. Government of Punjab*, 1981 SCMR 715, Supreme Court of Pakistan.

Act, with specific prohibition on integration of NADRA database for accessing data thereof without parliamentary authorisation.

5. Institutional Framework: NCEES, Judiciary, PFSA, Parliament

A National Commission on Electronic Evidence Standards (NCEES)⁵⁴ is to be established with powers to accredit AI systems and maintain a public accuracy register, audit all deployed Safe City FRT and ANPR systems annually, provide technical opinions to courts and report annually to Parliament. Tech-specialised judicial benches at High Courts and Sessions Courts trained in the Explainability Crisis, AEDS evaluation, drawing guidance jurisprudence evolved through Bridges/Williams/Puttaswamy are required to be constituted for technology-intensive cases. The PFSA and NFA must develop AI forensic audit capacity. The Personal Data Protection Bill is to be enacted, with 30-day data retention limits for FRT data of uncharged persons with prohibition on data of NADRA integration without authorisation. Pakistan should engage proactively with the OECD AI Principles⁵⁵, the UNESCO AI Ethics Recommendation 2021⁵⁶, and EU-UK bilateral AI audit cooperation⁵⁷ frameworks. This will position Pakistan as a regional leader in South Asian AI accountability standards.

⁵⁴ Proposed by the author as a dedicated regulatory body, the National Commission on Electronic Evidence Standards (NCEES) would be responsible for formulating and auditing the forensic protocols for AI-driven surveillance and algorithmic evidence in Pakistan.

⁵⁵ OECD, "*Recommendation of the Council on Artificial Intelligence*", OECD Legal Instruments, available at: <https://www.oecd.org/en/topics/sub-issues/ai-principles.html> (accessed March 14, 2026).

⁵⁶ UNESCO, "*Recommendation on the Ethics of Artificial Intelligence*", adopted on 23 November 2021, available at: <https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence> (accessed March 14, 2026).

⁵⁷ Tony Blair Institute for Global Change, "*Exploring EU-UK Collaboration on AI: A Strategic Agenda*", available at: <https://institute.global/insights/tech-and-digitalisation/exploring-eu-uk-collaboration-on-ai-a-strategic-agenda> (accessed March 14, 2026).

Conclusion

This article has argued that Pakistan's three-pronged algorithmic surveillance apparatus FRT criminal identification, ANPR penalty generation, and NADRA biometric integration is operating in unconstitutional territory across all three dimensions simultaneously. The black box problem structurally defeats Article 10-A's meaningful defence standard. The NADRA function creep violates Articles 9 and 14 without parliamentary authorisation. ANPR's automatic penalty generation without pre-issuance challenge or accuracy disclosure reverses the constitutional presumption of innocence. The application of Article 164 QSO to AI-generated evidence may highlight potential gaps in existing safeguards relating to the transparency and reliability of algorithmic outputs.

The comparative evidence is unambiguous. The UK Court of Appeal held in *Bridges* that FRT deployment without a precise legal basis and equality impact assessment is unlawful. The UK Parliament reversed the computer reliability presumption after 700 wrongful convictions. The Indian Supreme Court held in *Puttaswamy* that biometric data collected for civil registration cannot be repurposed for surveillance without independent constitutional authorisation. The US *Williams* settlement established that FRT evidence requires independent corroboration before arrest. Pakistan's current framework falls below every standard that every comparable jurisdiction has established as a constitutional minimum.

The five proposals advanced in Part 6, the Algorithmic Evidence Disclosure Standard covering both FRT and ANPR, the statutory Right to Explanation with trade secret override in judicial proceedings, mandatory Algorithmic Impact Assessments, IFTA amendments with specific remedies, and the National Algorithmic Evidence Commission constitute a constitutionally grounded, comparatively validated, and practically achievable reform framework. The Balochistan Safe City Project, approved in February 2026, is the last opportunity to build accountability in by design. For every citizen who passes through Pakistan's camera-covered cities from Lahore to Karachi, Islamabad to Peshawar, and now Quetta their constitutional rights under Articles 9, 10-A, and 14 depend on whether Pakistan chooses to govern its algorithms, or to be governed by them.