Journal of International Law & Human Rights
ISSN (Print): 3007-0120 ISSN (Online): 3007-0139
Volume 5, No.9, 2026, 79-89
DOI: https://doi.org/ 10.59075/jilhr.v5i9.338
Journal Homepage: http://journals.centeriir.org/index.php/jilhr

Digital Surveillance and Right to Dignity A Case-Study of Pakistan in light of Constitution and Islamic Jurisprudence

Bushra Zeb Khan[1], Dr. Naseem Razi[2]

[1]Lecturer, Department of Law, University of Malakand Email: khan.bushrazeb@gmail.com
[2]Associate Professor, Department of Law, International Islamic University, Islamabad
Email: naseem.razi@iiu.edu.pk

Abstract

The paper explores the capacity of the constitutional and legal framework of Pakistan, together with the Islamic legal norms, to regulate the use of artificial intelligence-enabled digital surveillance and to safeguard the right to privacy and dignity as well as the fair trial rights. The paper uses case law-based approach to explore the legal reasoning of the superior courts in the cases of Shehla Zia v WAPDA (1994), Mohtarma Benazir Bhutto v President of Pakistan (1998), the concurring opinion of Syed Mansoor Ali Shah J in Qazi Faez Isa litigation, Ishtiaq Ahmed Mirza v Federation of Pakistan (2019), Islamabad High Court in Pakistan Federal Union of Journalists (2022) and order of the Islamabad High Court (2024) on the Lawful Intercept Management System which was subsequently suspended by the Supreme Court. The legal reasoning in these cases is analyzed in the light of the constitutional provisions of Articles 4, 8, 9, 10A, 14, 19, 19A, 2A and 227 of the Constitution and the legal provisions of the Investigation for Fair Trial Act 2013, the Prevention of Electronic Crimes Act 2016 and relevant telecommunication laws. The paper also incorporates the Qur'anic and prophetic prohibition of spying and the maqasid al-shari'ah. The paper argues that the core principles for the limitation of the use of AI-enabled surveillance (legality, necessity, proportionality, independent authorization and effective remedy) exist in the law of Pakistan and these principles are in line with the Islamic requirements. The major problem is not the lack of standards but the implementation of these standards, limited scope of existing laws and the lack of any reported judgment on the use of artificial intelligence or algorithmic systems. Finally, the paper proposes a working framework for applying the existing judicial and Islamic tests on the use of AI-enabled surveillance.

Keywords: Artificial intelligence, digital surveillance, privacy, right to dignity, fair trial, Islamic jurisprudence, maqasid al-shari'ah, Pakistan

© 2026 The Authors. Published by Center of Innovation in Interdisciplinary Research (CIIR). This is an Open Access Article under the Creative Common Attribution Non-Commercial 4.0

Article History: Received: 02-10-2026 **Accepted:** 03-11-2026 **Published:** 05-11- 2026

Corresponding Author's Email ID: khan.bushrazeb@gmail.com

Introduction

Artificial intelligence and digital surveillance have enhanced the actual capacity of the Pakistani state to monitor, identify and classify individuals. It is possible to conduct mass surveillance on telecommunication networks. It is possible to match faces with large databases. It is possible to use automated tools to identify individuals for further investigation. The Constitution of the Islamic Republic of Pakistan 1973 addresses these developments and declares that "the dignity of man and, subject to law, the privacy of home, shall be inviolable".[1] It also guarantees the rights to life, liberty, fair trial and freedom of expression.[2] Articles 2A and 227 require that these rights must be interpreted in accordance with the Injunctions of Islam as laid

down in the Qur'an and Sunnah.[3]

The paper is concerned with whether the principles established by the superior courts, in the light of the governing laws and Islamic norms, are sufficient to regulate the use of AI-enabled surveillance or whether there are gaps in enforcement and legal structure which make the constitutional rights not effectively protected.

The main argument is that the core standards for the limitation of the use of AI-enabled surveillance (legality, necessity, proportionality, independent authorization and effective remedy) exist in the constitutional law of Pakistan as interpreted by the superior courts. These standards are in line with the Islamic requirements. The problem is not the lack of principle. The problem is the lack of implementation of the existing safeguards, the limited scope of the existing laws and the lack of judicial or legislative engagement with the specific characteristics of the automated systems.

Research Methodology

The research in this paper is mainly conducted through qualitative doctrinal research, which is then supplemented by normative analysis based on Islamic jurisprudence. The primary method of research used in this paper is case-law analysis. This involves close reading of the superior courts of Pakistan in the cases of Shehla Zia v WAPDA (1994),[4] the legal defects in the unregulated telephone tapping in the case of Mohtarma Benazir Bhutto v President of Pakistan (1998),[5] the personal scope of privacy and the consequences of the secret surveillance in the separate note of Syed Mansoor Ali Shah J in the Qazi Faez Isa litigation,[6] the evidentiary requirements for audio and video recordings in the case of Ishtiaq Ahmed Mirza v Federation of Pakistan (2019),[7] freedom of expression in the case of Islamabad High Court in Pakistan Federal Union of Journalists (2022)[8] and the order of the Islamabad High Court (2024) on the Lawful Intercept Management System.[9] These are analyzed in the light of the legal provisions of the discussed in Investigation for Fair Trial Act 2013, the Prevention of Electronic Crimes Act 2016, relevant telecommunication laws[10] and the Qur'anic and teachings of the Prophet against on spying in the light of the maqasid al-shari'ah. Since there is no reported judgment in Pakistan on the use of artificial intelligence or algorithmic surveillance, the paper further analyzes the application of the existing rules on legality, necessity, proportionality, independent authorization and remedy to AI systems by comparison.

[1]Constitution of the Islamic Republic of Pakistan 1973, art 14(1).
[2] Constitution of the Islamic Republic of Pakistan 1973, arts 4, 9, 10A, 19 and 19A.
[3] Constitution of the Islamic Republic of Pakistan 1973, arts 2A and 227(1).
[4] *Shehla Zia v WAPDA* PLD 1994 SC 693.
[5] *Benazir Bhutto v President of Pakistan* PLD 1998 SC 388.
[6] *Justice Qazi Faez Isa v President of Pakistan* PLD 2021 SC 1 (Constitution Petition No 17 of 2019), separate note of Syed Mansoor Ali Shah J. The note is cited below by its own paragraph numbers.
[7] *Ishtiaq Ahmed Mirza v Federation of Pakistan* PLD 2019 SC 675.
[8] *Pakistan Federal Union of Journalists v President of Pakistan* (Islamabad High Court, W.P. No 666 of 2022, Athar Minallah CJ, short order of 8 April 2022).
[9] Order of the Islamabad High Court (Babar Sattar J) dated 25 June 2024 in the audio leaks petitions of *Bushra Bibi and Mian Najam-ul-Saqib* (W.P. No 1805 of 2023 and connected petitions) („Audio Leaks Order"),

The paper is structured as follows. The constitutional framework is explained in Part 2. The main judgments on dignity, privacy and surveillance are analyzed in Part 3. The set of laws is reviewed in Part 4. The application of the case law to AI-generated or AI-processed evidence is analyzed in Part 5. The application of the case law to freedom of expression is analyzed in Part 6. The Islamic perspective is developed in Part 7. The analysis is synthesized in Part 8. The gap between principle and practice is identified. A working framework for the regulation of AI-enabled surveillance is proposed.

Constitutional framework

Article 14 on dignity and privacy

Article 14(1) makes dignity absolutely unconditional and makes the privacy of home inviolable "subject to law". This means two things. First, dignity is not subject to law. No law can authorize any act which offends dignity. Second, "subject to law" does not mean that the legislature or executive has a free hand. Article 8(2) says that the State "shall not make any law which takes away or abridges the rights so conferred". Any such law shall be void to the extent of such contravention.[11] Therefore, a power of surveillance is only valid if the law which creates it is itself in line with Article 14. As shown in Part 3, the courts have interpreted this right to go far beyond a physical house.

Articles 4 and 9 on lawful treatment, life and liberty

Article 4(1) says that "to enjoy the protection of law and to be treated in accordance with law is the inalienable right of every citizen" and of any other person in Pakistan. Article 4(2)(a) prohibits any act which is detrimental to "the life, liberty, body, reputation or property of any person" except in accordance with law.[12] Article 9 says that "no person shall be deprived of life or liberty save in accordance with law".[13] These provisions enforce a legal standard on the executive. Surveillance is not an inherent executive power. It must be based on a law which is clear, specific and valid.

Articles 10A, 19 and 19A on fair trial, expression and information

Article 10A (inserted by the Eighteenth Amendment) gives a person the right to "a fair trial and due process" in the determination of civil rights and obligations and in any criminal charge.[14] Surveillance has an indirect effect on these provisions. It may taint the evidence used in the trial of a person. It may also deter people from speaking.

Article 19 protects freedom of speech and of the press. This is subject to reasonable restrictions enforced by law on the grounds mentioned in the Article. Article 19A gives every citizen the right of access to information on matters of public importance. This is subject to regulation and reasonable restrictions enforced by law.[15]

Govt Hands ISI Keys To Mass Surveillance System" *The Friday Times* (Lahore, 9 July 2024)

<https://www.thefridaytimes.com/09-Jul-2024/govt-hands-isi-keys-to-mass-surveillance-system> accessed 30 September 2026.

[10] *Investigation for Fair Trial Act, 2013* (I of 2013); *Prevention of Electronic Crimes Act, 2016* (XL of 2016); *Telegraph Act, 1885* (XIII of 1885); and *Pakistan Telecommunication (Re-organization) Act, 1996* (XVII of 1996).

[11] Constitution of the Islamic Republic of Pakistan 1973, art 8(2).

[12] Constitution of the Islamic Republic of Pakistan 1973, art 4(1) and (2)(a).

[13] Ibid, art 9. [14] Constitution of the Islamic Republic of Pakistan 1973, art 10A, inserted by the Constitution (Eighteenth Amendment) Act 2010, s 5.

Articles 2A and 227 on Islamic frame

The Objectives Resolution (which is made a fundamental part of the Constitution by Article 2A) and Article 227(1) (which says that "all existing laws shall be brought in conformity with the Injunctions of Islam as laid down in the Holy Quran and Sunnah")[16] mean that the constitutional rights in Pakistan are read together with the Islamic norms. Therefore, the Qur'anic and prophetic prohibition of spying is treated as part of the framework for understanding in Part 7. It is not a separate moral appendix.

Judicial authority on dignity, privacy and surveillance

Shehla Zia v WAPDA: life includes dignity

In the case of Shehla Zia v WAPDA, which was about a grid station near the houses in Islamabad, the

Supreme Court gave a broad interpretation to Article 9. It held that "life includes all such amenities and facilities which a person born in a free country is entitled to enjoy with dignity, legally and constitutionally".[17] Although this case is not about surveillance, it is relevant for two reasons. First, it connects Article 9 with dignity in Article 14. Second, it treats the possibility of harm to the way of life of a person (not only actual harm) as a constitutional concern. These two ideas are relevant for AI systems. The harm of AI systems is widespread and difficult to see.

Mohtarma Benazir Bhutto v President of Pakistan: telephone tapping

The important precedent is the case of Mohtarma Benazir Bhutto v President of Pakistan. The petitioner (former Prime Minister) alleged that she was herself a victim of telephone tapping. The Court examined the practice in the litigation on the dissolution of her government. The Court found the practice unlawful and observed: "In our country, hardly there is any effective law, to check this menace and illegal act. No procedure has been established for regulating the tapping, taping or eavesdropping of private or official telephones. We find that tapping of telephones and eavesdropping of any person is reprehensible, immoral, illegal and unconstitutional act."[18]

There are three aspects of this decision which are important. First, the Court treated the lack of a regulating law as a constitutional defect itself. It did not treat it as a license for the executive to act. Second, the Court addressed the gap by directing that, until the Parliament legislates on the matter, the tapping must be done with prior permission from a commission or the Supreme Court on a case-by-case basis. The permission shall not be given for more than six weeks.[19] Third, the Court connected the tapping with privacy, Article 9 and the spirit of Islam.[20] Subsequently, the Parliament passed the Investigation for Fair Trial Act 2013, which is discussed in Part 4.

[15] Constitution of the Islamic Republic of Pakistan 1973, arts 19 and 19A. Article 19A was also inserted by the Constitution (Eighteenth Amendment) Act 2010.

[16] Constitution of the Islamic Republic of Pakistan 1973, art 227(1); see also art 2A and the Annex (Objectives Resolution).
[17] *Shehla Zia* (n 4) (Saleem Akhtar J).
[18] *Benazir Bhutto* (n 5), as quoted in Omer Imran Malik, „Tapping Phones" *Dawn* (Islamabad, 9 September 2022) <https://www.dawn.com/news/1709185> accessed 11 October 2026

Justice Qazi Faez Isa v President of Pakistan: privacy attaches to the person

The litigation in the case of Qazi Faez Isa was about a Presidential Reference against a Supreme Court judge. It was based on information collected by the Asset Recovery Unit in the Prime Minister's Office. The Court quashed the Reference. Syed Mansoor Ali Shah J concurred with the result. However, he wrote a separate note. He gave different reasons for the result. He dissented from the directions issued in the Short Order. Therefore, his note is a persuasive opinion. It is not the holding of the Court. However, it is the most developed judicial statement on surveillance in Pakistan.[21]

He wrote the following on the difference between investigation and surveillance: "While regular inquiry and investigation is limited to reaching out to lawful and visible evidence existing at the time, secret surveillance and interception are modern intrusive investigative tools for discovering and creating evidence against a person by encroaching upon his privacy and personal liberty."[22]

He wrote the following on the scope of Article 14: "Privacy attaches to the person and not to the place where it is associated. Home under Article 14 of the Constitution is not only the physical house but the entire treasure of personal life of a human being. The intrusion by the State into the sanctum of personal space, other than for a larger public purpose, is violative of the constitutional guarantees."[23] This interpretation is what makes Article 14 applicable to the digital tools. A person's messages, location, face,

browsing history, etc. are part of "the entire treasure of personal life" whether they are in a house or not. He also identified the social harm which is multiplied by the monitoring on the AI scale: "Undue surveillance can lead to a chilling effect on those critical of State institutions and societal norms."[24]

On the legal basis for surveillance, the note holds that "any secret surveillance or interception of the citizens of Pakistan other than under IFTA is starkly offensive to their fundamental rights of privacy and personal liberty",[25] and that, outside the limited sphere the statute covers, "the right to privacy is absolute, until law is enacted to regulate it. Absolute right entails absolute prohibition on its violation."[26] The note also listed thirteen principles drawn from international practice, among them legality, legitimate aim, necessity, adequacy, proportionality, judicial authorisation, due process, notification, transparency and independent oversight, and presented them as the human-rights approach to surveillance.[27] Those principles are a ready-made test for AI systems.

The note also identifies thirteen principles of human-rights-focused surveillance practices internationally (legality, legitimate aim, necessity, adequacy, proportionality, judicial authorisation, due process, notification, transparency and independent oversight) which can serve as a test for AI systems.

[19] Malik (n 18), summarising the interim directions issued in *Benazir Bhutto* (n 5).
[20] *Benazir Bhutto* (n 5).
[21] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, para 2.
[22] Ibid, para 27.
[23] Ibid, para 31, relying on *Benazir Bhutto* (n 5) for the meaning of „home" in art 14.
[24] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, para 32.
[25] Ibid, para 37.
[26] Ibid, para 48; see also para 38.
[27] Ibid, paras 33 and 36, drawing on the International Principles on the Application of Human Rights to Communications Surveillance, (2013).

The audio leaks order and the Lawful Intercept Management System

In the audio leaks proceedings (Bushra Bibi v Mian Najam-ul-Saqib) the single judge (Babar Sattar J) of the Islamabad High Court examined the mechanics of the leaks. His order of 25 June 2024 noted that the Pakistan Telecommunication Authority had required telecom licensees to install a Lawful Intercept Management System (LIMS) through which around 2% of subscribers (over 4 million people) could be monitored simultaneously.[28] The court observed that „such mass surveillance system seems inspired by George Orwell"s „1984""[29] and that „over the last 11 years since the enactment of the Fair Trial Act, not one surveillance permission has been sought from the courts in accordance with the provisions of the Fair Trial Act".[30] It concluded that „the LIMS has been installed and is being operated without any backing of the law, and those who are using and/or enabling the use of the LIMS to surveil citizens may have rendered themselves liable to criminal liability under provisions of the Fair Trial Act, Telecom Act, Pakistan Electronic Media Crimes Act (PECA), Telegraph Act and Pakistan Penal Code".[31]

The court rejected the national security argument for a closed hearing, stating that „National security, however, is not the security of an inanimate monolith. It is the collective security of the citizens to be protected by the state."[32] This and the previous passages apply the Benazir Bhutto logic to the modern telecommunications infrastructure and, specifically, to the LIMS which is exactly the kind of platform on which AI analytics could be run.

The order is not currently binding authority because the federal government appealed under Article 185(3) and, on 19 August 2024, a two-member bench of the Supreme Court (Aminuddin Khan J presiding) suspended the High Court orders of 29 May and 25 June 2024 and restricted the High Court from proceeding further. The value of the order, however, remains as a record of facts disclosed to the court and as reasoning on the constitutional limits of mass interception.[33]

What the cases establish

These cases, taken together, establish five propositions: (1) privacy and dignity are fundamental rights which apply to persons, not only to places; (2) surveillance must be clearly authorised by law and the lack of a regulating law is a ground for restrictt not a licence for the executive (Benazir Bhutto, Mansoor Ali Shah note); (3) when a statute does authorise surveillance, the procedure must be followed (the High Court‟s findings as to the unused warrant regime demonstrate that it was not); (4) surveillance has a chilling effect which extends to expression and the independence of the judiciary; (5) a court may decline to act on evidence which was obtained by unlawful surveillance. These propositions do not turn on the technology used and they apply to AI.

[28] Audio Leaks Order (n 9).
[29] Ibid, as quoted in *The Friday Times* (n 9).
[30] Ibid.
[31] Ibid.
[32] Ibid; see also „Surveillance state‟ *The News* ((Islamabad, 3 July 2024) <https://www.thenews.com.pk/print/1205749-surveillance-state> accessed 16 october 2026
[33] *Government of Pakistan v Bushra Bibi* (Supreme Court of Pakistan, Aminuddin Khan and Naeem Akhtar Afghan JJ, order of 19 August 2024), reported in Abdullah Momand, „SC suspends IHC order in audio leaks case, bars court from further proceedings‟ *Dawn* (Islamabad, 19 August 2024) <https://www.dawn.com/news/1853303> accessed on 16 october 2026

The Statutory Framework

Colonial and telecommunications statutes. Section 5 of the Telegraph Act 1885 permits interception „on the occurrence of any public emergency, or, in the interest of the public safety‟.[34] Section 54 of the Pakistan Telecommunication (Re-organization) Act 1996 permits the interception of calls and messages and the tracing of calls „in the interest of national security or in the apprehension of any offence‟.[35] Neither is specific, nor do they provide the procedural protections of the Fair Trial Act. SRO 1005(I)/2024, issued by the Federal Government in July 2024 under section 54, authorises officers nominated by the Inter-Services Intelligence to intercept calls and messages.[36] It was issued only days after the High Court noted that no rules had been framed and no permission granted under these provisions. It is the executive responding by notification, not legislation. Whether a notification under section 54 without the legislative safeguards is consistent with Articles 4, 9 and 14 is a question which the courts have yet to determine.

Investigation for Fair Trial Act 2013. This is the only statute providing for a full warrant regime. As summarised in the Mansoor Ali Shah note, the procedure involves the notified officer obtaining the permission of the Federal Minister for Interior and then a warrant from a judge of the High Court. Section 8 details what must be included in the application; section 10 details what the judge must consider; section 14 limits a warrant to 60 days, section 15 permits departmental action against an officer who makes an arbitrary request; section 35 provides for criminal liability for unlawful surveillance.[37] The Act is limited in its scope to scheduled offences such as terrorism. But it is significant in showing that the Parliament accepted that there should be prior judicial control over surveillance. The High Court‟s finding that the warrant regime was not used for 11 years is a finding of non-compliance with the Act, not a defect in the Act.[38]

Prevention of Electronic Crimes Act 2016. PECA creates offences (including unauthorised interception (section 19) and offences against the dignity of a natural person (section 20)). It also creates powers: the requirement for service providers to retain traffic data for a minimum period (section 32), the Pakistan Telecommunication Authority‟s power to remove or block „unlawful on-line content‟ (section 37), and the power of a court to order the real-time collection and recording of information on the application of an authorised officer (section 39).[39] PECA was amended in 2025.[40] For the purposes of this paper, the key point is structural. PECA provides the State with access to data on a scale which makes algorithmic analysis possible. However, there is no provision for automated processing, profiling or biometric identification.

Duties of confidentiality and data. Other statutes impose duties on officials who hold personal data. The

Mansoor Ali Shah note mentions section 28 of the NADRA Ordinance 2000 (which prohibits NADRA employees from communicating information which they acquire in the course of their employment) and section 216 of the Income Tax Ordinance 2001 (which protects tax records). It held that officials who had passed such data to the Asset Recovery Unit had breached their duties.[41] These provisions demonstrate that personal data in State databases is held on trust and cannot be moved around at will. This is directly relevant to the issue of sharing databases for facial recognition. At the time of writing this paper, no comprehensive personal data protection statute had been enacted.[42]

[34] Telegraph Act 1885, s 5(1).
[35] Pakistan Telecommunication (Re-organization) Act 1996, s 54(1).
[36] Notification SRO 1005(I)/2024 (Ministry of Information Technology and Telecommunication, 8 July 2024), issued under s 54 of the Pakistan Telecommunication (Re-organization) Act 1996; see *The Friday Times* (n 9).
[37] Investigation for Fair Trial Act 2013, ss 3(g), 8, 10, 14, 15 and 35; *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, paras 34-36 and 39.
[38] Audio leaks order (n 9).
[39] Prevention of Electronic Crimes Act 2016, ss 19, 20, 32, 37 and 39.
[40] Prevention of Electronic Crimes (Amendment) Act 2025 (Act No II of 2025).

AI, Evidence and the Right to a Fair Trial

The best current basis for assessing AI-generated or AI-processed material is the Supreme Court‟s guidance on audio and video evidence in Ishtiaq Ahmed Mirza v Federation of Pakistan. The Court collected the requirements which precedent requires to be met before a recording can be relied upon. They include: „(i) No audio tape or video can be relied upon by a court until the same is proved to be genuine and not tampered with or doctored. … (v) Accuracy of the recording must be proved and satisfactory evidence, direct or circumstantial, has to be produced so as to rule out any possibility of tampering with the record.“[43]

The Court added that the recording must be the actual record of the event; that the person who made it must be produced; that safe custody must be proved; that the source and date of acquisition must be disclosed; and that late production of a recording „may be looked at with suspicion“.[44] These rules were formulated for tapes but almost word-for-word they apply to deepfakes, synthetic voices and edited video which are the first AI risk which courts will face. A court applying them would require forensic proof of authenticity; a witness to explain provenance; and an unbroken chain of custody.

The related question is facial recognition. A match is a probabilistic output of a model, not an observation by a witness. Under Article 10A, the accused is entitled to know how the match was arrived at and to contest it. In practice, this means disclosure of the system used; the error rates; the quality of the image; and the database searched. If the identification is based on a watchlist, the accuracy of the list is as important as the accuracy of the match. There are no specific rules in Pakistani law of evidence for such outputs. The Ishtiaq Ahmed Mirza principles of genuineness, accuracy, provenance and proof would have to be applied by comparison, with expert evidence under the Qanun-e-Shahadat Order 1984.[45]

The separate note in Qazi Faez Isa case adds the exclusionary dimension. After reviewing the position in common law and comparative law, Mansoor Ali Shah J stated, „I concur in the principle, and see no hindrance in adopting it in our jurisdiction“ (viz. that evidence obtained by deliberate breach of constitutional rights is generally inadmissible because to admit it „would compromise the integrity of the judicial process“).[46] He went further, however, where there is no law regulating the intrusion. The right is then absolute and the exclusion of the evidence is This is not yet the law of the Court, but it is a coherent basis for the exclusion of AI-derived evidence obtained by unlawful bulk surveillance.

[41] National Database and Registration Authority Ordinance 2000, s 28; Income Tax Ordinance 2001, s 216; *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, para 38.

[42] The Personal Data Protection Bill 2023 was approved by the Federal Cabinet in July 2023 but has not been enacted by Parliament.
[43] *Ishtiaq Ahmed Mirza* (n 7), para 11, as reproduced in *Khanzadi v The State* (Sindh High Court, Omar Sial J, Criminal Appeals Nos 722, 723 and 661 of 2019), para 8.
[44] *Ishtiaq Ahmed Mirza* (n 7), para 11, requirements (vi), (vii), (xv), (xviii), (xix) and (xx).
[45] Qanun-e-Shahadat Order 1984, arts 59 and 164.
[46] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, paras 41-47.

Freedom of Expression and Access to Information

The Islamabad High Court (Athar Minallah CJ) in Pakistan Federal Union of Journalists v President of Pakistan struck down the Prevention of Electronic Crimes (Amendment) Ordinance 2022 and the criminal defamation element of section 20 of PECA. The short order held that the Ordinance was „promulgated in derogation of the Constitution and the fundamental rights guaranteed thereunder, particularly Articles 9, 14, 19 and 19-A".[48] The Court observed that absolute as well.[47]

„[f]reedom of expression is a fundamental right and it reinforces all other rights guaranteed under the Constitution of the Islamic Republic of Pakistan" and that „[f]ree speech protected under Article 19 and the right to receive information under Article 19-A are essential for development, progress and prosperity of a society and suppression thereof is unconstitutional and contrary to the democratic values."[49]

Although the case was concerned with defamation, the reasoning as to the chilling effect applies equally to surveillance and to automated content moderation. When people believe that their communications are being monitored, they self-censor (as noted in the Mansoor Ali Shah note).[50] This effect is felt most acutely by journalists, academics and activists. Article 19A introduces a transparency element which is rarely invoked. A citizen cannot challenge the system if he cannot learn that, for example, a system such as LIMS exists, or what data a facial recognition programme contains. Thus, the right to information should be interpreted as requiring the disclosure of the legal basis for, scope of and oversight of, State surveillance systems, subject to narrowly drawn security exceptions which a court can review.

The Islamic Perspective

The Qur'an

The Qur"an states that spying and having unfounded suspicion is forbidden. "O you who have believed, avoid much [negative] assumption. Indeed, some assumption is sin. And do not spy or backbite each other" (49:12).[51] The Qur"an also protects the home from spying and states that one must ask for permission to enter another person"s home. "O you who have believed, do not enter houses other than your own houses until you ascertain welcome and greet their inhabitants. That is best for you; perhaps you will be reminded. And if you do not find anyone therein, do not enter them until permission has been given you" (24:27-28).[52] The Qur"an also states that requests made to the Prophet"s wives must be done from behind a partition (33:53).[53] Finally, the Qur"an states that dignity is given to humans because they were created by Allah. "And We have certainly honored the children of Adam" (17:70).[54]

[47] Ibid, para 48.
[48] *Pakistan Federal Union of Journalists* (n 8), as quoted in Usama Khilji, „Some relief" *Dawn* (Islamabad, 10 April 2022) <https://www.dawn.com/news/1684304> accessed 20 october 2026.
[49] *Pakistan Federal Union of Journalists* (n 8), as quoted in IFEX, „Pakistan: Islamabad High Court strikes down PECA ordinance" (April 2022) <https://ifex.org/?p=332969> accessed 28 octobr 2026.
[50] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, para 32.
[51] Qur"an 49:12 (Sahih International translation, as for all Qur"anic quotations in this paper).
[52] Qur"an 24:27-28.
[53] Qur"an 33:53.
[54] Qur"an 17:70.

A further set of verses address the issue of AI-assisted decision-making. The Qur"an states "do not pursue that of which

you have no knowledge. Indeed, the hearing, the sight and the heart about all those (one) will be questioned" (17:36).[55] This means that a person must investigate a matter before acting on it. The Qur‟an further states "if there comes to you a disobedient one with information, investigate, lest you harm a people out of ignorance and become, over what you have done, regretful" (49:6).[56] This means that a person must investigate any information that is given to them by a disobedient person before acting on it. Thus, an algorithm that is used to flag a person without explanation, or a facial match that is accepted without human checking, goes against the duty to investigate before acting. Finally, the Qur‟an commands rulers to "render trusts to whom they are due" and "to judge with justice" (4:58).[57] Thus, State power over personal data is a trust, and not ownership.

The Sunnah

The Sunnah is consistent with the above Qur‟anic verses. The Prophet, peace be upon him, warned against spying and eavesdropping, stating: "Beware of suspicion, for suspicion is the worst of false tales, do not spy, and do not eavesdrop" (translation of the sense).[58] He further stated that the person who looks into a house without permission has no complaint if the householder repels him, and that asking permission to enter is prescribed because of sight.[59] A report in Sahih al-Bukhari states that whoever listens to the conversation of people who dislike it will have molten lead poured into his ears on the Day of Resurrection.[60] Another narration, reported by Abu Dawud from Mu„awiyah, who was himself a ruler, records the Prophet‟s warning that if you seek out people‟s faults you will corrupt them, or come close to corrupting them.[61] On the issue of harm, the maxim "there shall be neither harm nor reciprocating harm" is traced to a hadith and is among the foundations of the legal maxims.[62] On the issue of accountability, the Prophet said that every person is a shepherd and is responsible for those under his care.[63]

Classical fiqh and siyasah shar‘iyyah

These issues have been dealt with in classical fiqh and in the siyasah shar„iyyah. The home is inviolable and the ruler and his inspectors may not search a house on the basis of a suspicion of wrongdoing that is concealed. Al-Ghazali held that a wrong that is concealed behind closed doors is not to be investigated by means of spying, in the context of the duty of commanding right and forbidding wrong.[64] In the context of the muhtasib, Al-Mawardi limits the muhtasib‟s powers to search for wrongs that are manifest, and to investigate concealed wrongs on the basis of reliable information of a grave and imminent offence.[65] A report is attributed to „Umar ibn al-Khattab in which he had climbed over a wall to search for wrongdoers that he himself had exceeded the limits of his powers.[66] These authorities support the three conditions for intrusion into a home: concrete grounds before intrusion, a narrow purpose, and the official‟s accountability for his actions. inside a house, and found

[55] Qur‟an 17:36.
[56] Qur‟an 49:6.
[57] Qur‟an 4:58.
[58] Sahih al-Bukhari, no 6066; Sahih Muslim, no 2563 (narrated by Abu Hurayrah). Hadith numbers follow the sunnah.com numbering.
[59] Sahih al-Bukhari, nos 6241 and 6902; Sahih Muslim, no 2158.
[60] Sahih al-Bukhari, no 7042 (narrated by Ibn „Abbas).
[61] Sunan Abi Dawud, no 4888 (narrated by Mu„awiyah).
[62] Sunan Ibn Majah, no 2340 (narrated by „Ubadah ibn al-Samit); *Majallah al-Ahkam al-‘Adliyyah* (1876), art 19.
[63] Sahih al-Bukhari, no 893; Sahih Muslim, no 1829 (narrated by „Abd Allah ibn „Umar).
[64] Abu Hamid al-Ghazali, *Ihya’ ‘Ulum al-Din*, Kitab al-Amr bi‟l-Ma„ruf wa‟l-Nahy „an al-Munkar.
[65] Abu al-Hasan al-Mawardi, *al-Ahkam al-Sultaniyya*, chapter on *hisbah*.

Maqasid al-shari‘ah

The objectives of the Shari„ah are to protect religion, life, intellect, lineage and property. These are often listed as four objectives but some scholars include honour or dignity („ird) as a fifth objective.[67] A

technology is assessed by its effects on these ends. Mass surveillance of people in secret is contrary to the objectives of protecting dignity and freedom of the intellect. A system that makes consequential decisions about people without giving any explanation of how the decision was arrived at can pose a risk to life and property when it errs. The maxim al-darar yuzal (harm must be removed)[68] and the prohibition of unjust suspicion require that harm be prevented and remedied. At the same time the maqasid also include the preservation of life and public order and so the Islamic tradition does not prohibit all investigation, provided that it is necessary, proportionate and supervised.

Reading the Islamic sources with the Constitution

The test for the use of surveillance by the state can be derived from the Constitution as well as from the Islamic sources and it is almost identical to the legality, necessity, proportionality and oversight principles listed in the Mansoor Ali Shah note.[69] The test is three-part: 1) there must be clear and specific legal authority for the surveillance; 2) the surveillance must be necessary and proportionate to a legitimate aim such as the prevention of a grave crime; 3) there must be independent supervision of the surveillance and a remedy for any misuse. This test is almost identical to the test that can be derived from the Constitution and from the Islamic sources and is therefore the main argument of this paper.

Analysis: Protection, Gaps and a Working Framework

In relation to the protection offered by the constitutional and Islamic sources, there is strong protection. However, there are also weaknesses in the enforcement of the principles and in the lack of any rules in relation to the use of AI. The High Court, in the Benazir Bhutto case, found that no warrant had been sought under the Fair Trial Act in eleven years. This is a very serious weakness. The Supreme Court, in that case, did suspend the order but that does not mean that there is any confidence that there will be enforcement of the principles in the future. The lack of any personal data protection statute is also a serious gap. It means that there is no right for citizens to know what data is held about them, to have it corrected or to complain to an independent authority. PECA and the telecommunications statutes authorize the collection of data but do not contain any rules in relation to the automated analysis of such data. There are no reported judgments in relation to the use of facial recognition or in relation to the use of AI to make decisions about people.

[66] The report is cited in the literature on *hisbah* and in commentaries on Qur‟an 49:12; see, eg, Isma„il ibn Kathir, *Tafsir al-Qur'an al-'Azim*, on 49:12.
[67] Abu Hamid al-Ghazali, *al-Mustasfa min 'Ilm al-Usul*, on the five necessities (*al-daruriyyat al-khams*); Muhammad al-Tahir Ibn „Ashur, *Maqasid al-Shari'ah al-Islamiyyah*.
[68] *Majallah* (n 62), art 20.
[69] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, para 36

On the basis of the cases and sources examined above, the following is a working framework for any State use of AI-enabled surveillance.

1. Legality: All systems of surveillance must be authorized by statute which must name the purpose of the system, the data to be processed, the agency to use the system and the safeguards to be put in place to prevent misuse.[70]
2. Necessity and proportionality: The State must show that there is no less intrusive means of achieving the purpose of the surveillance and, in relation to bulk collection of data, there is a presumption that such collection is disproportionate.
3. Independent authorisation: The model of the warrant under the Fair Trial Act, 2013, with prior judicial approval and of short duration, should be extended to any new system of surveillance and enforced, with statistics published on its use.
4. Human review and explanation: No consequential decision about a person can be made on the basis of an automated output alone. A trained official must review the output and be able to give reasons for the decision, in accordance with the Qur‟anic duty to investigate before acting (49:6).
5. Contestability and disclosure: A person affected by an automated system of decision-making must be able

to learn that such a system was used and to challenge its accuracy, in accordance with Article 10A and Ishtiaq Ahmed Mirza.

6. Data protection: Parliament must enact a comprehensive data protection law with an independent regulator, purpose limits, retention limits and rights of access and correction.
7. Remedy and exclusion: Unlawfully obtained or unverified AI-derived evidence must be excluded and officials who breach the rules in relation to the use of such evidence must be held liable for their actions, in accordance with section 35 of the Fair Trial Act.[71]

Conclusion

Pakistan‟s Constitution, the leading judgments of the superior courts and the Islamic sources are in complete agreement on the core principle: the State may not spy on the people in secret without clear legal authority, a justified purpose, independent supervision and a remedy. This is the principle which was applied in the Benazir Bhutto case, in the separate note of Syed Mansoor Ali Shah J in the Qazi Faez Isa case and in the recent 2024 order of the Islamabad High Court in the audio leaks petitions of Bushra Bibi and Mian Najam-ul-Saqib. It is also the principle which the Supreme Court applied in the Ishtiaq Ahmed Mirza case to the use of evidence generated by AI. The problem is not the lack of principle; the problem is the lack of enforcement of the principles which have already been established. The most developed statements of the relevant principles are in the form of separate opinions or in the form of suspended orders of the superior courts. No court has yet applied the relevant principles to the use of AI by the State. The next step is for Parliament to legislate on the matter and for the courts to apply the existing tests to the use of AI by the State in the first case which comes before them.

Disclosure of AI Use

We did not use any generative AI tools to draft, outline, or develop the core ideas, analysis, or arguments of this paper. We did use a premium version of Grammarly for grammar and spell- checking. We also used ChatGPT, Claude and Gemini to rephrase and improve the clarity and flow of existing sentences that we wrote. We reviewed and edited all AI-assisted text in the paper and take full responsibility for the final content.

[70] *Qazi Faez Isa* (n 6), Syed Mansoor Ali Shah J, paras 37-38.
[71] Investigation for Fair Trial Act 2013, s 35.

References

1. Al-Ghazali, A. H. (n.d.). Ihya‟ „Ulum al-Din.
2. Al-Mawardi, A. al-H. (n.d.). al-Ahkam al-Sultaniyya. Constitution of the Islamic Republic of Pakistan. (1973). Investigation for Fair Trial Act, 2013 (Pak.).
3. Ishtiaq Ahmed Mirza v. Federation of Pakistan, PLD 2019 SC 675. Justice Qazi Faez Isa v. President of Pakistan, PLD 2021 SC 1.
4. Mohtarma Benazir Bhutto v. President of Pakistan, PLD 1998 SC 388. Ms. Shehla Zia v. WAPDA, PLD 1994 SC 693.
5. Pakistan Federal Union of Journalists v. President of Pakistan, Islamabad High Court (short order of April 8, 2022).
6. Prevention of Electronic Crimes Act, 2016 (Pak.).
7. The Qur‟an. (n.d.). Verses 4:58, 17:36, 17:70, 24:27–28, 33:53, 49:6, 49:12.