HJRS HEC Journal Recognition System Category Y

Vol 3 Issue 1 (July-Sep 2025)

ISSN (Online): 3006-4740

ISSN (Print): 3006-4732

Privacy of Home to Privacy-by-Design: Article 14 of the Pakistani Constitution in the Age of AI Surveillance

Muhammad Shoaib Jamil (**Corresponding Author**)*

Lecturer, University of Management and Technology, Sialkot Campus

muhammad.jamil@skt.umt.edu.pk

Azhar Ali Dayal

LLM Scholar, Grand Asian University Sialkot, azharalidayal@gmail.com

Huma Bilal

Lecturer, Political Science & IR, Grand Asian University, Sialkot, huma.bilal@gaus.edu.pk

Muhammad Noaman Qaiser

LLM Scholar, Grand Asian University of Sialkot, noamanwahla47@gmail.com

ABSTRACT

The constitutional right to privacy is more than ever challenged as Pakistan moves beyond targeted interception to advanced surveillance using analytics. This paper holds the view that the concept of the informational privacy against AI-controlled state surveillance as the target of Article 14 of the Constitution of Pakistan, which has traditionally guaranteed the dignity of the person and the privacy of the home, should be interpreted dynamically. As a doctrinal approach, the paper considers the Supreme Court precedents and the constitutional rights to due process (Article10A) and information (Articles 19 & 19A). Other major laws that we consider are the Investigation for Fair Trial Act (2013) and the Prevention of Electronic Crimes Act (2016). Based on these sources, we come up with a structured article 14 AI Surveillance Test which must have legal clarity, a legitimate purpose, necessity, data minimization, and independent oversight. The examples of the Safe City program on facial-recognition and telecom data retention under PECA demonstrate the application of the test and reflect severe constitutional flaws in the current regimes. Findings suggest that urgent legal and regulation changes are needed to make the surveillance technologies reflective

of the fundamental rights of Pakistan, such that the security improvements should not compromise the constitutional rights.

Keywords: AI surveillance, Article 14 (Pakistan), human dignity, privacy rights, Safe City projects, facial recognition, data retention, personal data protection

1. Introduction

Pakistan is undergoing a transition towards ambient, analytics-driven surveillance as compared to targeted interception communications. In the last ten years Safe City initiatives across the world have deployed several thousands of CCTV cameras to key cities that have automatic number plate recognition (ANPR) and face recognition (**Adil, K. 2018**). Similarly, surveillance organizations have increased digital surveillance: Telecom companies have been forced into a central interception system, which led to centralized interception by the authorities that permit the accessing of any user information or listen to their call. The emergence of privacy reforms heightens the need to define the privacy protection. In July 2024, the government officially permitted the ISI, made up of military personnel to intercept telephone messages and calls in the name of national security which made many question whether the interception will be abused and breach of constitutional rights will take place. (**Abbas, Z. 2024**). Meanwhile, provincial governments are trialing AI-tech-inspired recognition systems. As an example, the Safe City Authority in Punjab, in liaison with the police IT wing, has deployed an AI-driven Face Trace System (FTS) which crawls on live CCTV streams and compares the faces against databases comprising tens of millions of government-held identity records (**Abbasi, S. 2024**). The developments pose the doctrinal question, how is Article 14, in its guarantee of privacy, to regulate AI-enabled surveillance?

The application of article 14 is read purposely and considering the supreme court precedent and it does not just safeguard privacy in the home but also privacy outside it such as the privacy of communications, metadata, and personal data footprint (**Ahmed, N. 2021**). This understanding has already found the reflection in the jurisprudence of the Supreme Court. In a well-known Benazir Bhutto case (**1998 PLD SC 388**), the Court has explained that with regards to surveillance methods such as eavesdropping and phone-tapping this infringes on the fundamental right of privacy and inflicts harm to dignity. The Court also stated that privacy is not restricted to the dwelling area and illegal encroachments even in the immediate society or public areas is forbidden, so as to maintain the dignity of the person. In an earlier Suo motu proceeding with regards to the bugging of the phone of a judge, the Court compared telephone conversations to those conducted at home being under the aegis of Article 14, and termed that it cannot be listened to telephone conversation-wise, unless it is of absolute necessity and reasonable and to the extent permissible by law. Collectively, these precedents provide the understanding of the fact that AI-enabled surveillance is prima facie engaging rights. The existence of technologies which constantly track such individuals in their activity, movement, or even correspondence is a violation of the privacy of the home privacy guarantee even in a case where there is no physical entry of the home. Therefore, state use of AI surveillance will only be permissible in a regulated calculability assessment under Article 14. We shall contend that the constitutional system of Pakistan already has the instruments of such a test: the interpretation of Article 14, taking together the right to due process (**Article 10A**), the freedoms of expression and information (**Article 19 & 19A**)

provide the criteria that AI surveillance measures must fulfill. Concisely, AI-driven surveillance should be constitutional provided the surveillance action is legal, essential, proportionate and fair.

Methodology

In this article, doctrinal research is used to fill the gap between the language of Article 14 to modern period technologies of smart surveillance. We read the text of the constitution and follow its jurisprudential footsteps; codify statutory restrictions under the Pakistani surveillance legislation (in particular, the Investigation for Fair Trial Act 2013, the Prevention of Electronic Crimes Act 2016, and the Punjab Safe Cities Authority Act 2016); and extrapolate a multi-prong legal test that can be used to evaluate the surveillance regime in the face of fundamental rights violations. The proposed test is applied to two case studies, that is, real-life implementations of (a) facial recognition as applied in Safe Cities and (b) mass retention of telecom related information. The methodology will ensure the analysis is connected to real practices and is a practical illustration of how the suite principles of privacy-by-design can be applied to the Pakistani legal system.

2. Article 14's Text and Trajectory

Article 14(1) of Pakistan's Constitution says: "*The dignity of man and, subject to law, the privacy of home, shall be inviolable.*"

This implies two aspects are safeguarded at utmost point; human dignity and privacy. Dignity is not relative- it is unlimited. Privacy, however, is subject to regulation, which is under the law. However, it does not mean that the state has a blank license to interfere; any legal restriction to privacy, unless reached the level of fairness and need, will fall due to the pertinence of Article 8.

The fact that privacy is put parallel to a dignity indicates that privacy is not merely a concern of home protection as a physical entity, it is about the protection of personal dignity and independence. The dignity is accompanied by the individual, not by the property. That leads to a greater concept of privacy, which is not limited to the walls of a home, but involves personal information, communication, and life choices as well.

Courts Interpretations

Early case law in Pakistan interpreted the term literally in the privacy of home protection against incursion, both physically and forcefully. In the long term, the courts started to be more liberal in their living tree philosophy expanding the rights of privacy outside the house. They appointed judges to guard the information and messages about individuals due to the Indian court cases.

As an example, in 2004, the Lahore High Court held that the financial records of a bank customer are privileged and cannot be disclosed to another party without appropriate cause of action- although it is not the records of the bank which are retained in the home setting. (**PLJ 2004 Lahore 1147**) This indicated that the informational privacy also forms part of Article 14.

The Phone-Tapping Case

Mohtarma Benazir Bhutto vs. President of Pakistan (**PLD 1998 SC 388**) was the turning point. The case was on the issue of political phone surveillance. According to the decision made by the Supreme Court, phone tapping and eavesdropping constituted immoral, illegal, and unconstitutional behavior. It opined that such acts contravened privacy and dignity even without a statute prohibiting them and this means that right to privacy is directly under the Constitution.

According to the Court, a phone conversation was likened to conversation inside the house, which was worthy of protection. The case has been used to define the privacy law in Pakistan and communications have been given protection over any sort of surveillance. Subsequent cases established that privacy was a person, rather than a location, and that privacy was also in digital use and in public areas.

Why Dignity Matters

The words dignity of man in Article 14 fortifies the privacy rights. The Supreme Court regards infringements of privacy as a dig at dignity. The Article 14 may be violated when surveillance or data collection causes an under-represented individual to feel naked or demeaned or insecure. This is in tandem with the rest of world thinking in relation to human rights, including the UN understanding of ICCPR where it associates privacy with dignity (**Butt, A. (2024**).

This argument implies that the contemporary AI surveillance, such as one that follows the steps, biometrics, or online presence of a person, may potentially dare the dignity as much as traditional spying does, and thus must be subjected to rigorous legal scrutiny.

Recent Examples

The Supreme Court has yet to make a judgment on AI privacy but reflective of current cases, it appears that some concern exists regarding surveillance:

2012: Pakistan Telecommunication Authority (PTA) eavesdropped a talk between private late-night to support the blocking of particular call packages. Courts reminded that even the regulators had no right to evade the rule of law. (**Business Recorder, 2013**)

2023: The Islamabad High Court revealed how intelligence agencies had coerced telecom providers into installing a mass-surveillance system (LIMS) on not quite clear legal authority. (**Momand, Abdullah. 2024**)

Justice Qazi Faez Isa case (2019-2020): Secret surveillance was conducted on the judge and his family, access to personal data and travel records was gained and even foreign agents were said to have been tracking his children. Other people interpreted it to be illegal and against basic rights. (**PLD 2023 SC 661**)

Such events indicate courts are keen to be sensitive to the aspect of surveillance misuse and are potentially willing to take Article 14 to additional subtler forms of surveillance such as AI-based monitoring.

3. Statutory Framework

Surveillance Laws and Privacy Gaps

A number of legislations exist in Pakistan that authorize governmental surveillance. These encompass the laws concerning interception of phone and the internet, cybercrime, and the Safe Cities Authority. All these laws operate differently and offer varying degrees of safeguarding against privacy, and such that at times, they contradict the constitutional right to privacy under Article 14.

Investigation for Fair Trial Act 2013 (IFTA)

The IFTA (enacted 2013) is the first comprehensive Pakistan law governing targeted electronic surveillance. (**Daudpota, F. 2017**). It is aimed at legalizing but regulating the interception of communications, in the cases related to terrorism and national security, primarily. With IFTA, agencies like the ISI, IB and police are required to take a warrant granted by a judge in a High Court to intercept the communications of a person. Evidence and an appropriate authorization should be contained in the request. The definition of communication is intended to be wide indeed under the law. These include emails, SMS, internet records, call records, computer and mobile-based messages and even voice analysis. This implies that alternative means of surveillance have to be based on other legislation or run the risk of being unconstitutional.

Prevention of Electronic Crimes Act 2016 (PECA)

The law of cybercrime in Pakistan is known as PECA. The two more relevant sections to surveillance are Section 32 on mandatory data retention and Section 31 real-time data collection. (**Arshad Khan, E. 2018**). Under section 32, it is mandatory to ensure that all telecommunications companies, internet providers amongst, possess and maintain what is referred to as traffic data which must be maintained at least one year or on the other part, as stipulated by the Pakistan Telecommunication Authority (PTA). Traffic data refers to the metadata, which includes numbers dialed, calling time and duration of the call, IP addresses and location information.

Section 32 literally mandated the aggregation of a vast surveillance database with quite weak privacy safeguards, resulting in important Article 14 issues regarding whether retention of the communication records of the entire population is even justified and necessary.

Punjab Safe Cities Authority Act 2016 (PSCA Act)

Punjab Safe Cities Authority was enacted under the PSCA Act to incorporate modern-day technology in the policing structure within the province with Lahore as a pilot city and subsequently extending to other urban areas. (**Rana, M. A. 2024**). It enables the Authority to place CCTV cameras, construct control centers and incorporate communication systems to avoid crime, control traffic, and face emergencies. The open-ended powers contained in the PSCA Act can thus not pass the constitutional test on legality.

No General Data Protection Law

There is still no single piece of legislation that safeguards personal data in Pakistan. A Personal Data Protection Bill has been drawn up and been revised numerous times, lastly in 2023, but has not been enacted. The absence of the said law does not oblige government agencies to reduce data collection, seek consent, restrict processing to particular purposes, or endow individuals with their data rights. There are some sector specific regulations e.g. Telecom data under the PTA or citizen ID data under NADRA, but these are incomplete. That leaves privacy defense Article 14 and 8 of the constitution as the primary protection.

4. From "Home" to Informational Privacy

A Conceptual Shift

Right to Privacy of home is guaranteed in Article 14 of the Constitution of Pakistan. The conventional definition of this was safeguarding the intimate life of an individual in the physical sanctuary. In traditional times, homes were strictly considered as personal and what was considered to be public was visible to everyone. This method is unsuccessful when modern technology and AI surveillance is the order of the day (**Ahmed, Z. S., 2023**). In the same manner, phone, browsing and call data may be innocuous by itself. Concisely, AI eliminates the inherent restrictions that cushioned against the tracking of the activities of the people through time.

Privacy as Dignity and Autonomy

The Pakistani legal system has already progressed in the recognition of privacy that is not limited to the physical environments. Under Article 14, they have safeguarded phone calls, bank documents and other personal data in the country. This indicates that the privacy is associated with human dignity and free choice and not only with the home.

Why AI Surveillance Triggers Privacy Rights

Facial recognition systems, mass data analysis give the state the ability to view aspects of life that were not visible before. The cameras anywhere they are will recognize individuals who are in a political rally or religious shrine or where people come out to meet their friends (**Anwar, A., 2021**). This is capable of discouraging free speech and association which are also provided in the Constitution.

Metadata and Inferences Deserve Equal Protection

Previously, the law regarded the contents of a letter or a call as a piece of privacy but not the external information such as the address or the call timings. Nowadays, with the help of AI, it is possible to convert that external data into highly personal knowledge. As an example, information about whom you are calling/calling time would say something about your political affiliation or health conditions.

A New Standard for the AI Age

The concept of the privacy of the home stated in Article 14 can be interpreted as safeguarding the individual rather than the location. An example of privacy is the home and not the boundary of privacy.

Once the threshold is crossed, the state should establish that there has been a legal, reasonable, and proportionate surveillance to its end.

5. The Article 14 AI Surveillance Test

One of the methods through which the courts and regulators could determine whether AI-based surveillance agreement legitimates the constitutional right to privacy as specified in Article 14 of the Pakistan Constitution is by means of this test. It borrows on the provisions of the current Pakistani legislation such as the Investigation for Fair Trial Act (IFTA) 2013, but the approach is transferred into a contemporary technology. It is the concept of a feasible checklist that safeguards rights without prohibiting the vital security precautions.

This test applies in the determination by courts of a legal surveillance system (**Necessary and Proportionate. 2014**). It can assist regulators in the design of the systems to ensure that they do not violate the privacy initially.

Step 1 – Law and Clarity

The use of any AI surveillance should be expressly permitted by law. In article 14 it is stated that the right to privacy is safeguarded, which entails that the state may only infringe it upon the provision of appropriate legal grounds. The law should be explicit on the agency authorized to utilize the technology, in what manner, how, against whom and the procedure. Mere or indeterminate powers are insufficient.

Step 2 – Legitimate Purpose

There should be an adequate and significant purpose in the surveillance. Privacy is subject to limitation under the Constitution and any international law, such as on grounds of national security, the maintenance of public order, or to prevent crime. It should have a specific purpose though, rather than an abstract one.

Step 3 – Suitability

The technology should in reality serve its purpose to the intended purpose. It must be apparent that AI system can be used to attain its goal. Facial recognition applied in the capturing of terrorists should be precise enough to do so in the real-life context. The intrusive measures should not be justified in this manner that the technology is beneficial, but without evidence.

Step 4 – Necessity and Least Intrusive Option

A system should never be utilized even when it is functional unless there is an alternative less obtrusive method of attaining the same end. The state should establish that alternatives are not very effective. Likewise, it is more difficult to legitimize the data of all citizens long-term storage as compared to short-term storage or even just the suspect data.

Step 5 – Data Minimization

Only the necessary data should be collected and retained under surveillance. There should be no needless information being stored or kept eternally in it. This lowers the chances of abuse. The practical implications of this involve restricting what is recorded, blurring or anonymizing non-suspects, fast deletion of historic data and prevention of data being utilized beyond the strict reason in new legal consents.

Step 6 – Extra Care with Biometrics

In case of the system operating on biometric identifiers such as faces, fingerprints, or DNA, additional protection is necessary since these identifiers cannot be changed. To begin with, deployment of live facial recognition in society must require prior independent authorization, such as a warrant.

Step 7 – Fair Process and Rights

Article 10(A) the right to a fair trial and due process, and the right to information in Article 19A must be observed when the use of AI surveillance is adopted. Although the conduct of delicate functions may remain classified knowledge, people have the right to be informed of fundamental information regarding surveillance programs including the number of surveillance cameras installed, the nature of technologies applied, and general details on their efficacy.

Step 8 – Oversight and Accountability

Last, there should be some form of independent monitoring to ensure that all the precautions are taken. The controlling power may be on part of the courts, the parliament or a watch dog of privacy. The main fact is that it should not be the case that the very agency utilizing the type of technology conducts the review of itself.

Why This Test Matters

These eight steps are founded on the proportionality concept applied in most countries. This implies the balancing of the interest of the state to pursue a legitimate object against the interest to guard the basic rights. The test also introduces privacy-oriented specifically to AI, albeit rules, including avoiding bias, undesirable data gathering, and introducing biometrics information protection.

Table I Necessary and Proportionate Principles

Step	Key Question	What to Check
1 – Law and Clarity	Is there a clear and specific law allowing the AI surveillance?	Law names the agency, purpose, targets, and process. No vague or hidden powers.
2 – Legitimate Purpose	Is the goal specific, important, and lawful?	Purpose fits areas like serious crime prevention or counter-terrorism. No vague or political motives.
3 – Suitability	Does the technology actually	Evidence of accuracy and effectiveness under local

Step	Key Question	What to Check
	work for the stated aim?	conditions. Low error rates.
4 – Necessity / Least Intrusive	Is this the least privacy-intrusive method possible?	No alternative tool would work as well with less impact on privacy.
5 – Data Minimization	Is only the needed data collected and kept?	Unrelated data anonymized or deleted quickly. No extra use without new legal approval.
6 – Biometrics Safeguards	If using faces, fingerprints, or DNA, are there extra protections?	Prior approval, small watch-list, no mass scanning except emergencies, regular accuracy/bias audits.
7 – Fair Process & Rights	Can affected people challenge the surveillance?	Notification after safe period, right to contest, full logging, some public reporting.
8 – Oversight & Accountability	Is there independent oversight and real consequences for misuse?	Judicial, parliamentary, or watchdog review; annual reports; audits; illegal evidence excluded; programs stopped if non-compliant.

6. Application I: Safe City Facial Recognition under Article 14

This case study examines the application of facial recognition technology (FRT) in Pakistani Safe City projects, that is, Lahore in the Punjab Safe Cities Authority (PSCA) (**Anwar, A., 2021**). Thousands of CCTV cameras installed in Lahore since 2016 have been linked to a new command center. Artificial intelligence can be applied to the system to identify faces, read number plates on the vehicles and other security activities.

Step 1: Legality

In case of any invasive technology such as FRT it must have a defined basis in law. Neither the leading document of the creation of the Safe City projects, the PSCA Act 2016, nor its provisions imply facial recognition. The Act does provide the access to using the so-called modern technology to maintain public safety; however, this is a very generalized and ambiguous expression.

Step 2: Legitimate Aim

The Safe City FRT is meant to prevent crimes and counter-terrorism, as well as, to respond to danger with less time. Such goals are mostly considered within law as being valid. Finding an armed suspect or protecting a large event where a known terrorist was known to be present would be two acceptable applications.

Step 3: Suitability

The issue here is whether FRT can, in fact, contribute to the realization of the aforementioned objectives. Assuming that it could properly recognize the faces of the suspected individuals on watch-lists in real time, police could easily pursue them. However, when it results in excessive false matches or is prone to failure it is not as useful.

Step 4: Necessity

Necessity seeks to determine whether FRT is the less intrusive method of attaining the security goals. To illustrate, police might choose a specific surveillance to identify a suspect or distribute his picture among other officers without scanning the face of every citizen. Greater patrols or improved lighting could be an alternative, lessening the crime on the streets.

Step 5: Data Minimization

A privacy-friendly system is expected to collect and retain only the minimal amount of data. The Face Trace System in Lahore makes use of data about millions of citizens such as law-abiding drivers and residents in databases. It is also not clear how long data shall be stored and how they will be used in future.

Step 6: Biometric Safeguards

Facial recognition involves biometric data that is sensitive, therefore, special protections ought to be available. To switch on FRT, it does not have to obtain a warrant or authorization of an independent authority in Lahore. The system would seem to employ broad databases rather than watch-lists. Lacking these protective measures, the present system is not deemed to be of acceptable standards.

Step 7: Procedural Fairness

Procedural fairness implies that individuals, who are in the way of FRT, should have the right to contest its use. When an individual is erroneously detected and apprehended, he or she must be informed about using facial recognition and must be allowed to challenge such facial recognition in the court. In Pakistan, no process of this is presently in place.

Step 8: Oversight and Remedies

Safe City FRT has no independent oversight. The PSCA answers to the Punjab government which is at times taken over by the police themselves. It has no privacy commission and parliamentary review.

Overall Findings

The use of this test reveals that Safe City FRT as it is currently does, most likely, violate several aspects of Article 14. It lacks a clear legal foundation, it is non-targeted and non-specific, gathers too much information, and has no protection, control, and visibility.

What Reform Would Look Like

The government would have to enact transparent legislation or regulations to honor the rights to privacy. These should include that real-time FRT can be deployed only with a warrant of the High Court judge on the strong evidence that a suspect would be at particular location. Very focused watch-lists are to be small. These would ensure that FRT becomes more considerate of the rights of its citizens in that the system is built with their privacy being put first, instead of protection being built into it.

7. Application II

PECA Section 32 – Traffic Data Retention and AI Analytics

Case Overview

The case examines the constitutionality of the decision of the government to make telecom companies collect communication records of all people and maintain them over a prolonged time frame as stated in Section 32 of the Prevention of Electronic Crimes Act (PECA) 2016 (**Aftab, S. 2024**).

What Section 32 Says

Section 32(1) of PECA demands that service providers maintain some traffic information within a duration of one year. This can be prolonged by the government. The data should be maintained at its native form in order that it can be used as legal evidence. It implies that the state will be able to integrate live surveillance and historical data in order to develop a comprehensive portrait of the communication pattern of anyone.

Use of AI Tools

The use of AI and data analysis programs by agencies has increased their understanding of the expansive amounts of stored data. As an example, AI can determine which numbers are often in contact with the known criminals or which phones tend to be in the same location all the time implying meetings. With AI this would hardly be possible to discern anything like these patterns in so much data. Mass collection of data is permissible by section 32 and the AI facilitated easy use of such data in investigation.

Step 1: Legality

The first question under Article 14 is that is there a law, which authorizes this surveillance? Here there is a definite law; Section 32 of PECA. It is an alert to people which indicates that their metadata is kept at least a year. Yet the act is very general. It states that information has to be stored within a period which can be months or years or till the decision of the Authority, which effectively has no definite limit to it. Nevertheless, being a formal law enacted by the Parliament, it satisfies the minimum of the basics of the law.

Step 2: Legitimate Aim

The publicized intention of the government is to ensure that there is evidence that is available to probe crimes particularly cybercrime and terrorism. In the absence of compulsory retention, the service provider will be at liberty to remove the records promptly in order to cut the expenses rendering the inquiries more difficult. The police have acceptable goals such as national security and prevention of crime. The issue is that the law stores all data in order to use it at some point in time which would be prone to exceed what is actually needed. Nevertheless, the goal of crime prevention is acceptable in the framework of the analysis.

Step 3: Suitability

Access to previous traffic data can assist in solving crimes. Call records, location data, and internet logs have been utilized in most of the investigations. An example is that the investigators can determine whether two suspects were talking or whether a phone was in the vicinity of a crime spot. These searches are made quicker and more efficient with the use of the AI. Thus, form the usefulness point of view, retention of this information is helpful to law enforcement agency in accomplishing their goals.

Step 4: Necessity

The main issue in this respect is whether the minimum intrusive means to accomplish the target here would be retaining the information of all users at least with one-year expiry. Most likely no. There are alternative less-obtrusive means. This implies that necessary test of the law is not passed since this law is broader than necessary.

Step 5: Data Minimization

Minimization also implies that one should gather and retain only the required amount of data about a given purpose. Section 32 goes the contrary. It does not limit the variety of types of traffic data and makes it possible to use it in any investigation, including even the investigation of minor offences. This translates to the fact that the law does not meet the minimization requirement.

Step 6: Biometric Safeguards

This is primarily a measure regarding the security of biometric data such as fingerprints or facial photographs. The section 32 is not the case of biometrics, but metadata. Nevertheless, metadata may be highly sensitive since it can profile and fingerprint people. When metadata is utilized by AI to label humans as suspects, it is equivalent to casting judgments on them regarding sensitive areas. In Pakistan, automated decision-making has no policies; therefore, none is put in place to counter inaccurate decisions and biased targeting in such profiling.

Step 7: Procedural Fairness

Majority of the individuals are unaware of the fact that their information is being held in this minute detail. There exists no mechanism of alerting someone in case his data has been accessed by an agency. More recent judges have been prepared to challenge surveillance procedures and as a whole there can be little procedural fairness to citizens under the current regime.

Step 8: Oversight and Remedies

Monitoring of the used retained data is quite poor. Although, the Pakistan Telecommunication Authority (PTA) may play an indirect role and that too, with a government dependence. The operation of intelligence agencies is not publicly accountable. Courts have occasionally spoken about barring evidence gathered in an unlawful manner, however that is not an agreed-on principle.

Overall Constitutional Analysis

Under section 32, there is provision of mass collection of traffic data of all the telecom users in Pakistan. It is without discrimination as it perceives all people as possible suspects. This is opposed to the tenet of the constitutional right to privacy under Article 14. Stricter rules on retention could as well be imposed by regulators such as the PTA which are less probable without external force.

Chilling Effect and Free Speech

People can also censor themselves knowing that all of their calls, messages and internet usage are tracked. This could make them evade some conversations and topics even when legal due to fear of surveillance. This has an impact on the freedom of speech as established under Article 19 and the issue of privacy is even worse.

8. Anticipating Counter-Arguments

The Debate on AI Surveillance and Privacy

Any suggestion of robust privacy regulations regarding AI surveillance will be opposed. Skeptics and governments will propose that they are necessary to be surveilled to be safe. One should realize these arguments and answer appropriately.

“We Need These Tools for Security”

The government can respond that the country is faced with severe security issues such as terrorism, sectarian conflicts and organized crime. They will argue that it is necessary to have surveillance tools, mass CCTV and facial recognition to stop the attack or to arrest criminals. Legally, the basic rights cannot be overlooked even when the country is faced with a crisis of security unless there existed a well-declared emergency.

“Public Spaces Are Fair Game”

It is said that when you are out there, you have no right to privacy. They say that cameras just document things that can be viewed by anybody. However, this overlooks the fact that being under surveillance all the time is quite unlike general visibility in the society. Individuals would like to believe that their daily activities are not recorded in a governmental database unnecessarily.

“If You’ve Done Nothing Wrong, You Have Nothing to Hide”

This is a popular saying, which however is confused. Everyone has a right to privacy, not only people who are suspected in some crimes. People have diaries, curtains and guard their privacy on their personal information not because they are guilty of anything but because they believe in personal life. Indeed, the lack of restraint in surveillance may result in the country being less safe as its resources are spent on unrelated information and annihilate the faith that the state can be trusted.

"Safeguards Are Too Expensive or Slow Things Down"

Policymakers can state that there are security measures to prevent crimes such as warrants, audits, and supervision that are expensive and time wasting and hinder faster work. However, a lot of safeguards are cheap and simple to introduce into existing systems. In constitutional democracy, there must be certain procedural delays as inalienable aspect in rights.

"Pakistan's Threats Are Greater, So We Need More Freedom"

Arguably, Pakistan is more threatened than countries such as those found in Europe thus not to be subjected to rigid rules of privacy. Rights are the most relevant in situations of crisis whereas local contexts are more relevant in the common days. Pakistan is also a signatory to international conventions which include the International Covenant on Civil and Political Rights that mandate that it uphold the privacy.

Security and Privacy Can Work Together

All these anti-arguments fail to confirm that uncontrolled mass surveillance is needed. A system can be created wherein the safety and privacy is safeguarded. This is not a question of halting surveillance in general, but one of making surveillance justified and constrained. Defending privacy is not a weakness, but a feature of a responsible and effective state.

9. Doctrinal Outcomes and Recommendations

Practical Steps for Courts and Government

Besides the action we propose, should our analysis hold up, the courts and the government could undoubtedly take specific steps to ensure that AI surveillance is performed in accordance with the Constitution. Such measures concern court proceedings and government policy amendments and laws.

Role of the Courts

Article 14 of the Constitution entitles every person in the country with the right to informational privacy, which must be understood and acknowledged by the higher courts in Pakistan including the High Courts and the Supreme Court. Personal data would be safeguarded and surveillance in places other than the home should be shielded by this right. Clearing up these standards would create a powerful message to the police, observe the rules now, as judges will insist on warrants, safeguards and due oversight in the future.

Role of the Government and Regulators

The government should not just wait on the courts to take action. The executive and legislative branches can pursue a number of sensible measures that can help them to design surveillance system with a mind towards providing privacy. Regulations of the Punjab Safe Cities Authority and other such institutions should be revised to regulate the usage of facial recognition and other surveillance methods. The next step would be to pass a Personal Data Protection Bill. A certain degree of leeway may be added to cater to emergency. This maintains the equilibrium between fast response and securing privacy.

Balancing Security and Privacy

All the above steps are aimed at finding a compromise between upholding the rights of an individual and safeguarding the population. The courts as well as the government have a part to play. Effective surveillances must also be acted on real threats only, but not on unlimited surveillances or on innocent persons.

With such changes, Pakistan would follow other nations that are establishing privacy in their governance systems at an early stage. This would help the Constitution to live up to promise of inviolability of dignity and privacy despite the country embracing modern technologies.

10. Conclusion

The 1973 Constitution of Pakistan in Article 14, guarantees the human dignity and privacy, not only in the home but also communications and personal information. This right is needed in the era of AI surveillance more than ever. We propose an A14 AI Surveillance Test to ensure that surveillance is: lawful, necessary and limited, fair, and adequately monitored, in particular when it involves biometric data. When the practices are applied to a case such as Safe City facial recognition and blanket data retention, it is common to find them not living up to the standards. Pakistan should not abandon the use of AI in security however; it has to adhere laws stipulated in the constitution. This will safeguard the rights of people, earn the trust of the people and further enhance the effectiveness of security. Establishing good rules and regulation will help the country to make sure that technology and privacy will develop hand in hand and keep both security and freedom intact in the digital world.

References

Abbas, Z. (2024). The surveillance system keeping tabs on millions. *Dawn*.

Abbasi, S. (2024). Caught in the web: Surveillance, data protection and AI in Pakistan. *Dawn*.

Abdullah Momand. SC suspends IHC order in audio leaks case, bars court from further proceedings. August 19, 2024. https://www.dawn.com/news/1853303/sc-suspends-ihc-order-in-audio-leaks-case-bars-court-from-further-proceedings

Adil, K. (2018). Making Punjab Safe City Authority smarter. Courting the Law.

Aftab, S. (2024). Right to Privacy and Freedom of Expression in the Constitution of Pakistan. In: Comparative Perspectives on the Right to Privacy. Ius Gentium: *Comparative Perspectives on Law and Justice*, vol 109. Springer, Cham. https://doi.org/10.1007/978-3-031-45575-9_4

Ahmed, Zahid Shahab; Yilmaz, Ihsan; Akbarzadeh, Shahram & Bashirov, Galib. (2023). "Digital Authoritarianism and Activism for Digital Rights in Pakistan." *European Center for Populism Studies (ECPS)*. July 20, 2023. https://doi.org/10.55271/rp0042

Ahmed, Z. S., Yilmaz, I., Akbarzadeh, S., & Bashirov, G. (2023). Digital authoritarianism and activism for digital rights in Pakistan. European Center for Populism Studies.

Anwar, A., Waqar, B., Syed, M., Sajid, A., & Khan, M. (2021, June). The role of safe cities in increasing public safety & tackling rapid urbanization in Pakistan. Centre for Chinese Legal Studies, LUMS.
the_role_of_safe_cities_in_increasing_public_safety_tackling_rapid_urbanization_in_pakistan_0.pdf

Arshad Khan, E. (2018). The prevention of electronic crimes act 2016: An analysis. LUMS LJ, 5, 117.

Asghar, N. (2025). Capital to get AI-powered crime watch. The Express Tribune.

Associated Press of Pakistan. (2024). From blind murders to swift justice: AI sky eye elevates ICT to 93rd safest city with 2,700 arrests.

Benazir Bhutto v. Federation of Pakistan, PLD 1988 SC 416.

Bukhari, H., Haq, I., & Shakoori, A. R. (2023). Constitution and right to privacy. Business Recorder.

Business Recorder. Ban on night packages: Supreme Court admits mobile firms' appeal against IHC's verdict. September 26, 2013. https://www.brecorder.com/news/40383523/only-a-miracle-could-bring-capacity-charges-down-nepra

Butt, A. (2024). International covenant on civil and political rights (ICCPR). Available at SSRN 4856071.

Chaudhry, A. (2022). Lahore fails to accrue Safe City project potential. Dawn.

Constitution of the Islamic Republic of Pakistan. (1973). Article 14: The dignity of man and, subject to law, the privacy of home, shall be inviolable. Islamabad: Government of Pakistan.

Daudpota, F. (2017). Pakistan-Understanding Its Law on Electronic Surveillance and Interception. Available at SSRN 2960330.

Digital Rights Foundation. (2018). Punjab Government's Safe Cities Project: Safer city or over policing? Privacy International.

Express Tribune News Desk. (2024, July 4). Telcos running mass surveillance system under PTA's orders. *The Express Tribune*.

Human Dignity Trust. (2017). Justice K.S. Puttaswamy (Retd.) and Another v. Union of India & Ors – Supreme Court of India.

Iqbal, S. (2023). The right to be forgotten in Pakistan. International Bar Association.

Junaid, M. (2024). Firewalls and mass surveillance: Is Pakistan moving toward stricter digital censorship? Voicepk.net.

Moreham NA (2018) Remedies for breach of privacy. Hart Publishing

Necessary and Proportionate. (2014). International Principles on the Application of Human Rights to Communications Surveillance. https://necessaryandproportionate.org/files/en_principles_2014.pdf

Pakistan Kanoon. Dignity and privacy of home. Retrieved July 19, 2025, from https://www.pakistankanoon.org

Privacy International. (2019). State of privacy: Pakistan.

Privacy International. (2023). Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill.

Rana, M. A. (2024). Punjab Safe Cities Authority (PSCA)–A Review Case Study. https://www.researchgate.net/profile/Muhammad-Rana-11/publication/384637899_Punjab_Safe_Cities_Authority_PSCA_-A_Review_Case_Study/links/6700a64df599e0392fb67ce6/Punjab-Safe-Cities-Authority-PSCA-A-Review-Case-Study.pdf

Research Society of International Law. Electronic surveillance and interception laws in Pakistan. RSIL Law Review.

Research Society of International Law. Right to fair trial. RSIL Law Review.

Shahzad, A. (2024). Pakistan authorizes spy agency to intercept phone calls. Reuters.