ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

Artificial Intelligence, Facial Recognition and Government Data Practices in Pakistan (Analysing Privacy Risks under Article 17 of ICCPR and the HRC's 2024 Concluding Observations)

Tufail Ali Shaikh
tufail.shaikh98@gmail.com
Ph.D. Scholar (Law), International Islamic University, Islamabad
Corresponding Author: * Tufail Ali Shaikh tufail.shaikh98@gmail.com

Received: 02-11-2025 **Revised:** 24-11-2025 **Accepted:** 14-12-2025 **Published:** 23-12-2025

ABSTRACT

Pakistan is utilising Artificial Intelligence in many areas particularly in security and public administration. Tools for example facial recognition cameras, large identity databases and digital monitoring systems are growing common in various major cities. These technologies can assist in crime reduction and service delivery and they also create questions about right to privacy of person because Pakistan does not keep a strong and complete data safety law. Many people do not aware about how their private information is being gathered & store and also there are no visible available rules that can limit how government departments can utilise this data system. Pakistan is a party to the ICCPR and Article 17 of the ICCPR safeguards everyone's right to privacy. The United Nations Human Rights Committee reviewed Pakistan in HRC's 2024 Observations and showed views about the way digital systems are being utilised by public departments or bodies. . HRC's 2024 highlighted that facial recognition and other Artificial Intelligence devices may not have particular legal safety that Pakistan needs to make better laws, checks and transparency related to usage of AI tools/ devices. This research paper highlights how Pakistan utilises AI technologies particularly facial recognition and digital monitoring and analyses how these practices relate to Article 17 of the ICCPR. It explains the main thoughts about privacy, reviews available material on Artificial Intelligence and data safety describes Pakistan's digital environment and examines whether current practices meet international human rights standards or not. The paper also tells practical reforms that can assist Pakistan be benefitted from AI without harming people's rights to Privacy. The purpose is to show that technology can be helpful but only when it doesn't violate human dignity and privacy Rights in accordance with ICCPR AND HRC's 2024 concluding observations.

Keyword: *Artificial Intelligence, security, public administration, facial recognition cameras, large identity databases, digital monitoring systems, ICCPR, United Nations Human Rights*

INTRODUCTION

Artificial Intelligence has grown an essential part of government systems in various countries. It is being utilised to operate or organise identity records, keep camera networks system, assist police in searching out and manage public services.

Pakistan is moving in this direction too. Major cities of Pakistan such as Islamabad, Lahore, Karachi, and Quetta now they have large camera systems. These systems can know/check faces, read vehicle number plates and examine traffic flow system. NADRA organises a large biometric database that includes fingerprints, facial photos and family details of almost every citizen. Telecommunications companies also keeps private data record that can be assessed by authorities. All these tools involve form of data collection and analysis and most of them depend on Artificial Intelligence oriented technologies.

From These developments, it appears that Pakistan is becoming a digital society. But this also creates duty and liability upon the authorities. From the public, Many citizens do not know when their data is collected, why it is stored or who can assess or see and assess it. Pakistan does not have a complete data protection law yet that explains how people's information should be protected and handled.. Some departments can access personal information without a court order. There is little transparency about how long data is kept or how mistakes or errors can be rectified.. Because of this, people may feel that they do not have control over their own information, given to authorities.

As a member of the ICCPR, Pakistan should protect privacy under Article 17. This means that the government can only interfere with someone's privacy if it is based on a clear law, and the action must be necessary and reasonable according to law.. The UN Human Rights Committee, in its 2024 report on Pakistan, warned that some of the country's digital monitoring practices do not meet these standards. The Committee noted that Pakistan needs stronger and strict laws, better checking , and more about how Artificial Intelligence tools are being used.

Artificial intelligence systems are influential and authoritative. They can examine many thousands of faces in minutes. They can interconnect information from different kinds of available sources and predict behaviour. When gathered with big identity databases or telecommunications data, Artificial Intelligence can form complete profiles of a life of person along with where they go normally, who they gather or meet and what their habits or conducts are. Without stricts rules, these devices can raise impact not just privacy right of person but upon freedom of expression and freedom of movement as well.

The main aim of this research is to know how Artificial Intelligence technologies are being utilised in Pakistan and how they fit with the right to privacy standards of Article 17 of the ICCPR. The article goes through available existing studies, elaborates the legal framework relating to this issue and explores digital data practices of Pakistan. It also look at examples from Safe City projects, NADRA systems and telecommunications data access. The main goal is to know risks, know data record keeping system run and to give recommendations/suggestions that can help Pakistan utilise technology duty or liability and make sure the safety of rights to privacy of people.

At the moment, Pakistan is at that situation where Technology is being used or grown speedily. So the country wants to upgrade and update to meet the system at world level. This is a good chance and opportunity but the things is strong laws and protections related to privacy rights must also grow side by side with technology usage. . Privacy must not be superseded or left for the sake of progress. An equal effort is possible, where technology develops and grows but the important is public services also respecting human rights. This research hopes to provide support that balance by providing a clarity and simple explanation of the issues involved and faced by the general public/common people.

Perspectives on Artificial Intelligence and Right to Privacy

Study on Artificial Intelligence and right to privacy has developed speedily and rapidly from the past some years. Many a scholars, courts and human rights groups and activists have written about how modern technologies cause effect upon personal freedom and dignity of the people of the society. Their work assist us to understand the situation in Pakistan and why privacy concerns are being increased.

Many human rights organisations have studied facial recognition technology. Reports from Human Rights Watch and Amnesty International display that facial recognition can create mistakes particularly with women, children and dark skinned face individuals. They also highlight that the technology can be utilised

to look after or check peaceful gatherings or trace people in public without their knowledge. This creates challenges about the effect of Artificial Intelligence on freedom of expression and peaceful assembly.

A famous writer in this field is Shoshana Zuboff., she describes and explains how organisations gather personal information in silent and hidden ways and then utilise that information for different objects. . Despite the fact that she emphasises primarily on private companies, the same concerns also put into practice to government data practices. Her main point and concern is that people generally do not aware how much their information is being gathered about them.

The European Union has also initiated hard and strict rules for data safety . The General Data Protection Regulation is considered one of the strongest privacy laws in the world. It secures and gives rights to citizens and enforced duties or responsibilities upon organisations that receive or gather personal data. The European Union is also creating the Artificial Intelligence Act which puts special restrictions on high-risk Artificial Intelligence systems along with facial recognition in public spaces. Many countries in the world use these rules as a model for their own laws.

And also Courts in Europe have also played an important role. The European Court of Human Rights has passed/rendered judgments explaining that any form of monitoring or controlling system must have a direct and express legal basis. Court has also given guidelines or orders that such steps should be necessary and should not be overly broad or cross limit. These directions under decisions pay vital role and are helpful because they provide a detailed understanding that how privacy of the people should be protected under human rights law.

In South Asia, privacy discussion usually focus on national identity systems. For example, India's Aadhaar system came across with challenges in court related to amount of biometric information it gathered. . Researchers in Pakistan have also discussed about NADRA's database and the risks connected to saving sensitive information in one place. They state that without strong laws, biometric data can be misused, checked or can be said as approached without the consent of concerned person.

Civil society organisations in Pakistan have participated important research. The Digital Rights Foundation has discussed about the flaws in Pakistan's data safety environment and the need for stronger safety. Media Matters for Democracy has reviewed Safe City projects and pointed out several weaknesses in transparency and public awareness and information. The Human Rights Commission of Pakistan also shares annual reports that highlight privacy challenges and the speedy growth of digital systems without clear oversight and checking.

The 2024 Concluding Observations of the UN Human Rights Committee are also an important source. The Committee showed issues about Pakistan's utilise of digital monitoring and control systems and unavailability or absence of a adequate or proper data safety law. It highlighted that Pakistan should ensure that causing interference or intervention with privacy of person follows or comes under the standards of Article 17 of the ICCPR.

From this research and study , we can experience three major ideas. First AI and facial recognition have grown powerful tools that can cause effect on privacy of people. Second, strict laws and oversight systems checking are required to safeguard personal data. Third, Pakistan's current framework is not proper and adequate. It needs improvement to meet with the criteria and international standards as per the report.

THEORETICAL FRAMEWORK

The theoretical framework of this study is based on international human rights law, particularly Article 17 of the International Covenant on Civil and Political Rights. Pakistan has signed this treaty so it should adopt its rules. Article 17 of the ICCPR protects people from unnecessary or unreasonable interference with their personal life, including their data.

The United Nations Human Rights Committee which watches the ICCPR , states what Article 17 of the ICCPR actually means. One of its essential documents is General Comment Number 16. This document explains that governments should have clear laws before they gather or use personal information of the people. These laws shouldn be easy to know and understand and they should describe or explain when and why data can be gathered or collected. . It also highlights that any act that interferes or transgresses with privacy of the people should be necessary where it needs and should not go beyond what is required for a legitimate purpose and must not violate or cross the limit relating to privacy right of person.

This idea is particularly essential when we discuss about Artificial Intelligence. Modern AI tools can gather and examine information rapidly. Facial recognition can recognise people even when they are in a public place. When combined with other data, AI can make complete profiles about a person's behaviour, relationships and daily routines and conducts. . This forms Artificial Intelligence more over reaching than older technologies, hence stronger safeties are required to protect the privacy rights.

International human rights law also uses three tests to decide whether an interference of intervention with privacy is acceptable. These tests are:

Legality

There should be a obvious or direct law that permits the interference. The law should be available publicly. It must be precise and understandable. Unnecessary rules are not allowed.

Necessity

The interference must function for legitimate object like public safety. It must be truly needed for obtaining that aim.

Proportionality

The government must utilise the least intrusive method available. If a less harmful procedure can function then the government cannot use a more harmful one.

These tests are useful and beneficial for examining Pakistan's digital monitoring of control systems. Many systems function without available specific laws which creates problems and concerns about legality. If large amounts of data are gathered when it is not required or needed, the necessity test become fail. . And if systems saves too much information for long periods without a clear object they may be fail in the proportionality test.

The UN Human Rights Committee's 2024 concluding observations assesses of Pakistan adds further guidance. The Committee showed concern that digital and AI systems in Pakistan are growing or developing without proper safety and oversight. It observed and pointed out that Pakistan's data protection framework is weak and that surveillance like practices may cause effects to the rights of journalists, activists

and ordinary citizens. These observations help this research and tells why Pakistan needs stronger safeties and protections.

In general, the theoretical framework brings to our mind that privacy is not just a technical issue. It is a particular main human right. As Pakistan follows more Artificial Intelligence tools, it must make sure that dignity of people and freedom are protected. Technology must deliver the people their safety of right , not only control them. This is the core principle of Article 17 of the ICCPR and it helps the rest of this study.

Pakistan's Digital Monitoring and Government Data Practices

Pakistan has grown many systems that gather and utilise personal data of the people for security and administrative purposes. These systems are dependent on Artificial Intelligence particularly facial recognition, biometric databases and automated data analysis. While these technologies can guide to maintain order and develop government services, they also raise serious privacy challenges because there are no strong and clear ruling guiding how these tools should be utilised

One of the noteable developments is the Safe City projects in cities like Islamabad, Lahor, and Karachi. These types of projects use thousands of cameras installed in public places. Many of these cameras are linked or related to Artificial Intelligence software that can identify faces, detect vehicles, monitor traffic and track unusual activity. Police officers often depend or rely on these systems for investigations and inspections and for responding to emergencies.

Despite the fact that these systems can be useful and beneficial they act or function without a specific law that explains their purpose, limits or duties. Common people do not know and is not aware when their face is being scanned or checked or for how long the footage is possessed or kept. There is also no clear way for someone to know if their data is saved by mistake or how to rectify it. This creates questions and problems about transparency and accountability of the usage.

Like this , there is other major institution is NADRA which maintains one of the largest biometric databases in the world. It keeps or saves facial photos, fingerprints, addresses, and family details of millions of Pakistanis. This information is utilised for identity cards, passports, voting lists and welfare support programs. Since biometric data is extremely sensitive, any misusage can cause effects long term. Despite , Pakistan does not have a strong data protection law that explains how NADRA should save this information, when it may share it or how long it may keep or possess it. There have also been media reports about possible data leaking which raises public concern and challenges.

Telecom companies also gather personal data. They record call details, mobile locations and internet use patterns. Government authorities can take request this data for security aims. In some cases, data is checked without a court order. Again, the main problem or challenge is the lack of transparency. People are not informed when their data is checked, why it is accessed, or who assented the request of assessing.

Artificial intelligence is also being used in policing in some regions. Predictive policing software analyses old crime data to know the areas where crime may occur in the future. Despite the face that this can guide police to respond quickly but it also causes risks unfairly targeting certain neighbourhoods particularly poorer communities. Without checks and oversight, such tools can amount to discrimination.

Civil society organisations have showed concerns that journalists, activists and students may be checked or controlled through digital tools. Monitoring peaceful gatherings or scanning faces at rallies may restrict people from participating in public life. This can cause effect to local values and freedom of expression.

All in all, Pakistan's digital systems have developed speedily but the legal framework has failed to keep pace. Resultantly, many practices happen without clear rules, oversight or public awareness. This causes privacy risks that should be tackled in compliance with Pakistan's international obligations or responsibilities in terms of Article 17 of the ICCPR and as per General comment no. 36 and also HRC's 2024 concluding observations.

ICCPR ARTICLE 17 ANALYSIS

Legality, Necessity and Proportionality

Article 17 of the ICCPR safeguards the right to privacy. It tells that nobody should face unlawful or arbitrary interference or intervention with their personal life, home, or correspondence. For a government to interfere with privacy, it must adopt or make clear and specific rules. The Human Rights Committee uses three tests to decide if the interference is acceptable. These tests are legality, necessity, and proportionality.

Legality

To meet the legality requirement, there must be a specific law that describes when and how personal information can be gathered or monitored. The law must be available publicly and it must be easy to know and understand. It must also limit the powers of the authorities from transgressing or violating.

In Pakistan, many Artificial Intelligence devises used by public institutions do not have a clear legal basis. Safe City systems, facial recognition tools and predictive policing programs functions through administrative decisions not through acts of Parliament. Telecom data is checked or approached, based on internal methods instead of Clear laws. People do not know what data is collected, how it is used, or how long it is kept. This means Pakistan does not fully meet the legality requirement of Article 17 of the ICCPR.

Necessity

To meet the necessity requirement, the intervention should deliver a legitimate purpose and must be truly required for achieving that object. The government cannot gather data just because it is easy or convenient.

In Pakistan, data collection through Safe City cameras and telecom systems is often broad and not limited to specific threats. Facial recognition is sometimes utilised in general controlling even when there is no direct requirement. Telecom data may be checked for cases that are not so essential. These practices tells that the necessity requirement is not fully satisfied.

Proportionality

Proportionality means that the government must utilise the least intrusive method available. If a smaller step can achieve the same result, then the government must take the smaller step.

In Pakistan, large amounts of data are gathered, saved and sometimes shared without limits. Facial recognition can know hundreds of people in one scan even when they are not related to any criminal activity. Telecom data can show someone's daily routine and social relationships. NADRA holds permanent biometric information without clear deletion rules.

When these three tests are applied simultaneously , it becomes direct that Pakistan's digital data practices meet challenges in meeting the standards of Article 17 of the ICCPR. The Human Rights Committee's 2024 concluding observations repeat this concern and call for stronger safeties

CASE STUDIES

Case studies guides us showing how Artificial Intelligence and digital monitoring actually function in Pakistan. They make the problem easier to understand and know.

Safe City Facial Recognition in Islamabad

Islamabad's Safe City project utilises cameras connected to facial recognition software. These cameras scan faces in markets, roads, public square and also near sensitive buildings. However the system helps police identify suspects, it also gathers information about large numbers of common people. Since there is no clear law governing this system, people do not know how their images are used or stored. This creates privacy concerns.

NADRA Data Storage and Security

NADRA manages the national identity database, which contains biometric and family information. If this data is misused or leaked, people can suffer permanent harm. There have been media reports about unauthorised access to NADRA's systems. There is no strong law showing how violations should be reported or how individuals can ask help. This creates questions and challenges about security and accountability of the system.

Telecom Data and Location Tracking

Telecom companies save detailed call and location data. Concerned Authorities sometimes ask request this information for investigations. Although without judicial approval and proper checking , there is a risk that such data may be checked so easily. Location data can show where a person goes. who they meet with and how long they stop in certain places.

Artificial Intelligence Assisted Policing

Some police departments use software to know crime locations in advance. This software depends on old data, which may include bias. Resultantly, the same neighbourhoods may be approached repeatedly. This causes unfairness and may raised mistrust between citizens and police.

These case studies show how Artificial Intelligence systems can cause affect privacy of the people if they function without proper rules and laws.

FINDINGS

The main findings of this research are:

- Pakistan is adopting AI technologies rapidly but the legal framework does not match this developments..
- Government data practices lack transparency and oversight.

- There is no clear data protection laws that explains how personal data must be collected, stored or shared.
- Many AI systems do not meet the legality, necessity, and proportionality requirements of Article 17.
- Also there is limited public awareness about digital rights of person and how data is being used.
- The UN Human Rights Committee has stated clearly that Pakistan must develops its privacy safeguards system.

RECOMMENDATIONS

To protect privacy and meet international standards, Pakistan should consider the following measures:

1. Introduce a Strong Data Protection Law

The law should define what personal data is, explain rights of people, and set standards/rules for government bodies. It should cover biometric data and facial recognition.

2. Create an Independent Data Protection Authority

This authority should check how data is used, hear complaints of complainants and enforce penalties for misuse of that data and violation of the privacy rights.

3. **Regulate Facial Recognition Tools**

Real time facial recognition should only be used in serious cases and with court approval. The government should also publish how accurate the software is.

4. Improve Oversight of Telecom Data

Telecom data must only be checked/assessed with proper approval. Companies should publish annual transparency reports in order to create trust and follow the privacy rules as per the Article 17 of the ICCPR.

5. Increase Transparency in Safe City Projects

Authorities/concerned departments should inform the public how long they keep camera footage, where cameras are installed and how the data is protected.

6. Conduct Human Rights Impact Assessments and checking.

Before using AI tools, government departments should carry out privacy and human rights impact assessments.

These steps can help out Pakistan, to get benefit from technology without violating the rights of its people.

CONCLUSION

Pakistan is growing to digital future and Artificial Intelligence tools are being part of daily basis governance. These /devises can support public safety and improve government services. Without strong legal safeties, , they can also create harm to privacy of person. As a country that has signed the ICCPR, Pakistan must make sure that its digital practices follow the rules of Article 17. This requires clear laws, independent checking, and open communication with the common people..

Technology should be utilised to help society and common people, not to minimise individual freedom. By adopting proper laws and safeguards, Pakistan can find a balance and equal where innovation and human rights exist both.. Privacy is a fundamental right and protecting it is important for creating trust among people, their, dignity, and continuing democracy.

BIBLIOGRAPHY

Books

Crawford, Kate. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. New Haven: Yale University Press, 2021.

Lyon, David. Surveillance Society: Monitoring Everyday Life. Buckingham: Open University Press, 2001.

Richards, Neil, and Jonathan King. Big Data Ethics: The Law and Policy of Artificial Intelligence. Oxford: Oxford University Press, 2020.

Zuboff, Shoshana. The Age of Surveillance Capitalism. New York: PublicAffairs, 2019.

International Human Rights Sources

International Covenant on Civil and Political Rights (ICCPR), 1966.

UN Human Rights Committee. General Comment No. 16: Article 17 (Right to Privacy).

UN Human Rights Committee. Concluding Observations on Pakistan, 2024.

UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris: UNESCO, 2021.

Pakistan-Based Reports

Digital Rights Foundation. Privacy in Pakistan: Data Protection Landscape. Lahore: DRF, 2023.

Digital Rights Foundation. Cyber Governance and Rights in Pakistan. Lahore: DRF, 2022.

Human Rights Commission of Pakistan. State of Human Rights in Pakistan 2023. Lahore: HRCP, 2024.

Human Rights Commission of Pakistan. Digital Surveillance and Civil Liberties in Pakistan. Lahore: HRCP, 2024.

Media Matters for Democracy. Safe City and Digital Rights in Pakistan. Islamabad: MMfD, 2022.

Media Matters for Democracy. Digital Policing and Public Rights. Islamabad: MMfD, 2023.

NADRA. "Biometric Registration System: Operational Overview," Government of Pakistan, 2024.

Pakistan Telecommunication Authority. "Lawful Intercept Management System," PTA Notification, 2017.

International Civil Society Sources

Amnesty International. Digital Policing and Human Rights in Pakistan. London: Amnesty International, 2024.

Article 19. Surveillance, Privacy, and Freedom of Expression in South Asia. London: Article 19, 2023.

Human Rights Watch. Pakistan's Expanding Digital Monitoring Systems. New York: HRW, 2023.

Privacy International. Biometric Data and Human Rights Risks. London: PI, 2021.

Legal & Regulatory Frameworks

European Union. General Data Protection Regulation (GDPR). Brussels: EU Publications Office, 2018.

European Union. Artificial Intelligence Act (Draft). Brussels: EU Commission, 2024.

European Data Protection Board. Guidelines on Facial Recognition Technology. Brussels: EDPB, 2020.

Case Law

European Court of Human Rights. S. and Marper v United Kingdom, 2008.

European Court of Human Rights. Zakharov v Russia, 2015.