

The Digital Panopticon: Reconciling State Surveillance under PECA with the Fundamental Right to Privacy

Asma Hanif Sethi

LLB (School of Law), LLM (University of Lahore), DTL (PULC), DCLP (PULC).

asmausmansethi@gmail.com

ABSTRACT

As digital surveillance become increasingly common in Pakistan, this research objective is to explore the consequences on the right of an individual relating to the privacy given no well-defined legal framework. Although the Constitution purports to protect individual privacy and dignity, the absence of articulation of protection for digital and informational privacy has enabled unfettered state surveillance on individuals, especially under the Prevention of Electronic Crimes Act, 2016 (PECA). The lack of a comprehensive data protection law, confusing legalese and insufficient oversight by the courts have resulted in massive attacks on digital and human rights. This article illustrates how various democracies have managed to balance the imperative of safeguarding civil liberties while meeting legitimate demands for national security through resort to international norms and best practices. Saeed argues that the existing monitoring in Pakistan amounts to a digital Panopticon where people are observed all the time, often without their knowledge or remedy under law. It outlines reforms that may be pursued in the area of law, the judiciary and civil society after considering proportionality, necessity and legality. Because only by replacing a system of hegemonic authoritarian Fiat with one based on transparency, human rights and respect for the constitution can this transition take place.

Keywords: Privacy Rights, Surveillance, PECA, Constitution of Pakistan, Cyber Law, Fundamental Rights, Comparative Jurisprudence, Digital Panopticon

1. Introduction

The state could watch over its citizens in ways that were unimaginable just a few decades ago as society became more digital. The combination of new technologies

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

and the government's aim to protect citizens and maintain order instead has led from relatively surgical, targeted surveillance to massive spying on people with no reasonable cause. Pakistan has made it possible in accordance with its Prevention of Electronic Crimes Act, 2016 (PECA)¹. PECA is strictly speaking a criminal law provision that is used as an excuse for surveillance. Despite allegedly being passed to counteract online harassment, fraud, and terrorism, the broad language of PECA and its dearth or procedural safeguards have led to significant claims that fundamental rights primarily the right to privacy is being infringed on.² Pakistan's case of surveillance reminds us of the "Digital Panopticon" idea, first articulated by Jeremy Bentham and further expounded upon Michel Foucault. ³Under constant surveillance in the digital panopticon people begin to censor themselves, follow along with a given line of control, and their democratic freedoms wean gently off them. The situation approaches crisis in Pakistan which has no data protection law. This means that people are susceptible to government surveillance, but they can also be preyed on by corporation's data brokers and telecoms specifically⁴. Without any supervision they work in this open space and often it is without control and oversight, and of course no responsibility⁵. PECA gives state agencies the right to collect, intercept and retain consumer data without any court authorization; particularly the Pakistan Telecommunication Authority (PTA) and Federal Investigation Agency (FIA). Under PECA Sections 31 to 39, such powers include the power to collect traffic data, intercept communications in real time and block for extremely broad offence like morality or national interest. This lack of transparency, procedural accountability and adequate checks and balances in the legal rules allows

¹ Privacy International and Digital Rights Foundation, *State of Privacy in Pakistan* (Privacy International, 26 January 2019) <https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan> accessed 1 August 2025.

² Hija Kamran, *Privacy-in-Law: How Safe Is Your Data?* (Digital Rights Monitor, 27 September 2019) <https://digitalrightsmonitor.pk/privacy-in-law/> accessed 1 August 2025.

³ Hija Kamran, *Pakistan's Digital Panopticon* (GenderIT, 26 July 2024) <https://genderit.org/articles/pakistans-digital-panopticon> accessed 1 August 2025.

⁴ Sindhu Abbasi, *Caught in the Web: Surveillance, Data Protection and AI in Pakistan* (DAWN, 22 October 2024) <https://www.dawn.com/news/1864073> accessed 1 August 2025.

⁵ Random History Facts, *Surveillance and the Digital Panopticon: Historical Evolution, Contemporary Mechanisms, and the Struggle for Privacy and Autonomy* (A History Fact A Day, 20 June 2025) <https://ahistoryfactaday.org/surveillance-and-the-digital-panopticon-historical-evolution-contemporary-mechanisms-and-the-struggle-for-privacy-and-autonomy/> accessed 1 August 2025.

state power to function beyond constitutional protections.⁶ This contrasts sharply with the surveillance practices of democratic countries which are constrained by the principles of necessity, proportionality, legality and oversight. The application of these regulations services patterns of government motivated surveillance, targeting journalists, civil society contributors and opposition. There are documented examples of harassment, and data theft a risk is the risk of being exploited more clearly, especially in a context where press freedom is compromised and institutional independence fragile. ⁷However, in the absence of a dedicated digital rights regime by means to regulation like India, European Union or United States, there is not yet an explicit and thorough legal recognition of digital rights framework in Pakistan although judiciary has recognized privacy as constitutional concept under Article 14⁸. This article critically assesses the real-world employment of PECA as a state surveillance tool and argues for an alignment of such powers with constitutionally guaranteed privacy rights. It tries to set out the main elements of a tentative reform agenda based on relevant case law, comparative legal frameworks and theoretical considerations. It makes the case that Pakistan might devolve into a regime of constant surveillance, where democratic participation is restricted, opposition is suppressed, and privacy is reduced to a myth⁹, in the absence of significant legislative reform and institutional accountability.

2. The Legal Framework Governing Privacy in Pakistan:

Article 14(1) of the 1973 Constitution of Pakistan establishes the fundamental framework for privacy protection, stating:

*"The privacy of the home and the dignity of man shall be inviolable, and subject to the law."*¹⁰

While the provision itself does not use the key words 'data privacy,' 'digital privacy,'

⁶ Muhammad Fahad Ashfaq and Ihtisham ul Haq, *Data Protection Laws and Their Implications on the Fundamental Rights* (RCIL & HR) <https://rcilhr.com/data-protection-laws-and-their-implications-on-the-fundamental-rights/> accessed 1 August 2025.

⁷ Ethan Dettman, *Examining Pakistani Digital Surveillance and Privacy Rights* (Tech4Humanity Lab, Virginia Tech) <https://tech4humanitylab.clahs.vt.edu/?p=30> accessed 1 August 2025.

⁸ Constitution of the Islamic Republic of Pakistan, Article 14 – *Inviolability of dignity of man, etc.* (Pakistan Kanoon) <https://pakistankanoon.com/statutes/constitution-of-pakistan/article-14/> accessed 1 August 2025.

⁹ *Privacy-in-Law: How Safe Is Your Data?* (Digital Rights Monitor, published under the #PrivacyHumSabKe campaign, 2019) <https://digitalrightsmonitor.pk/privacy-in-law/> accessed 1 August 2025.

¹⁰ Constitution of the Islamic Republic of Pakistan 1973, Art 14(1)

or ‘informational privacy,’ by way of judicial interpretation that stems from a fundamental constitutional guarantee, it has been read to include such modern corruptions beyond the confines of one’s physical home.¹¹ It’s an expression of a more expansive human flourishing personal autonomy, freedom from arbitrary interference, and above all, control over our information at the enterprise level in a world gone digital. In *Benazir Bhutto v. Federation of Pakistan* (PLD 1988 SC 416), the Supreme Court first laid down as far back in 1988 a very broad interpretation of Article 14 allowing any technology to qualify for protection under this article. The Supreme Court of Pakistan, on the controversial subject of wiretapping (eavesdropping), and political surveillance held that unauthorized secret phone taps and spying on leaders or organizations without approval from courts is a serious violation in terms of defamation to dignity, privacy.

This Court noted that such activities when carried on by the State have to be circumscribed with legal safeguards which shall include prior judicial approval, following due process. The ruling was a reminder that government surveillance is subject to protections under the Constitution, particularly when it threatens personal freedoms.¹² Further in *Justice Qazi Faez Isa v. President of Pakistan* (PLD 2021 SC 1), In this high profile case, the Supreme Court dealt with the accusation of unwarranted scrutiny and publicizing of the tax and finance declaration of a serving judge of the Supreme Court. The Court criticized the interference by the state in the life of the individual and reassured that the privacy enjoyed by the individual is provided under Article 14 even by any public official. The court emphasized that the personal information, including tax records, are not to be revealed or retrieved by government on a non-legal basis. The Court condemned the political manipulation of the use of surveillance and the importance of institutional safeguards on these intrusions.¹³

3. Unresolved Gaps in Legal Doctrine

Although the above cases indicate a judicial recognition of digital and information privacy, the Pakistani judiciary has yet to codify these principles into actual

¹¹ *Digital Privacy in Pakistan: Ending the Era of Self-Regulation* (Shaikh Ahmad Hassan School of Law, LUMS) <https://sahsol.lums.edu.pk/node/17036> accessed 2 August 2025.

¹² *In Benazir Bhutto v. Federation of Pakistan* (PLD 1988 SC 416)

¹³ *Justice Qazi Faez Isa v. President of Pakistan* (PLD 2021 SC 1)

statutory norms or means of redress. There are no system restraints on:

- What counts as “reasonable” surveillance according to the constitution.
- Conditions under which state agencies can access digital communications or metadata.
- Procedural safeguards to be met prior to conducting surveillance or data collection (e.g., judicial warrants, time constraints, mechanisms for accountability)

Courts have not gone so far as to establish a particular test or standard for determining how much surveillance is lawful and unlawful in digital realm. In turn, this ambiguous opens the door for executive overreach. Because the reasonable reading of Article 14 by courts corresponds with international human rights norms which regard privacy as central to human dignity, freedom of expression and personal security. The absence of legislative clarity and institutional accountability further compromises the implementation of privacy rights on the ground in Pakistan, with PECA and similar laws under which the state can gain unprecedented levels of surveillance, the constitutional promise of privacy could be a dead letter without some sort of judicial protections.¹⁴

4. No Data Protection Law in Pakistan

In digital era, leaving apart cases of commercial profiling, law enforcement, political targeting and surveillance personal data rose as most valuable asset. This data should be protected as a democratic imperative, not a new luxury. Under pressure to address these concerns, countries globally have moved faster than the U.S. to put in place a comprehensive data protection regime that specifies what entities can collect personal data and for what reasons and under what kind of protections it must be held. Unfortunately, Pakistan remains an exception. There was no data protection law in Pakistan, as opposed to the General Data Protection Regulation (GDPR) of

¹⁴ Privacy International and Digital Rights Foundation, *State of Privacy in Pakistan* (Privacy International, 26 January 2019) <https://privacyinternational.org/state-privacy/1008/state-privacy-pakistan> accessed 2 August 2025.

Sahar Iqbal, *The Legal Landscape for Privacy and Surveillance in Pakistan* (International Bar Association, 20 June 2023) <https://prod-bo.ibanet.org/legal-landscape-for-privacy-surveillance-in-Pakistan> accessed 2 August 2025.

European Union or Digital Personal Data Protection Act, 2023 of India that would regulate how personal data of its citizens should be collected, stored, saved, processed and shared. This legislative gap leaves individuals open to mass surveillance, profiling and the misuse of power over sensitive information by both state and non-state entities.¹⁵

5. Failed Attempts at Legislation

Pakistan has distributed several drafts of a proposed Personal Data Protection Bill since 2018, with the latest being the Ministry of Information Technology and Telecommunication (MoITT) version in 2021. The bill creates a Data Protection Authority, sets out data subject rights (such as the right to access, rectification and erasure) and obligations on entities holding or processing data. But while those are promising provisions in it, the bill has received significant push-back for Over-zealously exempting government agencies, especially for national security reasons, failed to ensure that the surveillance or data access is authorized by a prior judicial authorization, without independent oversight (separation from the executive), and Vague, over inclusive terms like “national interest” that could be deployed to justify (almost) any data breach.¹⁶

As of August 2025, the bill remains unaccented and the Data Protection Authority is still, only a concept. Civil society organization, contextually Digital Rights Foundation (DRF) and Media Matters for Democracy both have time and again argued that the draft bill though a course correction is inadequate until it entails robust powers of enforcement, transparency obligations, or judicial redress mechanisms.¹⁷

6. Implications of the Legal Vacuum

The lack of a comprehensive data protection legislation in Pakistan also create implications with respect to state surveillance such as:

¹⁵ “Bill on Personal Data Privacy Gets Cabinet Nod” (*The Express Tribune*, 27 July 2023) <https://tribune.com.pk/story/2428142/bill-on-personal-data-privacy-gets-cabinet-nod> accessed 3 August 2025.

¹⁶ *Pakistan’s Digital Rights Organisations Submit Feedback on the Data Protection Bill to the Government* (Digital Rights Monitor, 23 September 2021) <https://digitalrightsmonitor.pk/pakistans-digital-rights-organisations-submit-feedback-on-the-data-protection-bill-to-the-government/> accessed 3 August 2025.

¹⁷ Tahir Amin, *IT Ministry Finalising Personal Data Protection Bill* (Business Recorder, 22 May 2024) <https://www.brecorder.com/news/40304612> accessed 3 August 2025

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

- **State Access without Limit:** No judicial oversight can possibly stand in the way of any law enforcement or intelligence agency demanding access to a user's data (emails, messages, location data) from telecom companies or social media platforms.
- **Lack of Transparency:** Citizens are not informed about when their data will be accessed, stored or shared by government which violates principles of informed consent and due process.
- **No Right to Challenge or Rectify:** Those whose information has been illegally obtained or used, do not have a clear right under the Act to challenge this illegal access and corrected.
- **The rise of a surveillance economy:** In the absence of regulation, private data brokers and marketing firms collect and sell data with zero restraints in what has become an informal surveillance economy.
- **Vulnerable to Abuse with Sensitive Contexts:** It's those that are marked in saree when activists, journalist and political opponents were once again under the highest risk without any statutory checks in place to prevent these from becoming weaponized by their own digital footprints.

Essentially, monitoring is made lawfully possible by this regulatory void. It gives the government and commercial organizations unfettered access to digital identities without the associated accountability. Agencies may keep, intercept, and distribute data in accordance with PECA Sections 29 to 32; but, in the absence of a data protection law, there is no legal barrier separating legitimate inquiry from capricious intervention.¹⁸

7. Comparative Perspective

By Contrast, in Most Other Jurisdictions

Compliance Over time, the European Union who set the bar for global data protection compliance with GDPR which came into force in 2018. It has stipulated that personal data processing must be “lawful, fair and transparent” and Consent is

¹⁸ “Pakistani telecoms’ murky policies put users’ privacy at risk: rport” (*Dawn.com*, 30 December 2016) <https://www.dawn.com/news/1305364> accessed 3 August 2025.

Zahid Shahab Ahmed, Ihsan Yilmaz, Shahram Akbarzadeh and Galib Bashirov, *Contestations of Internet Governance and Digital Authoritarianism in Pakistan* (International Journal of Politics, Culture and Society, 7 October 2024) <https://doi.org/10.1007/s10767-024-09493-2> accessed 3 August 2025.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

central. For Individuals who can request your data from the site (make an access request) and ask us to rectify or erase your personal data. Even a state surveillance has to be proportionate, necessary and time-bound.¹⁹ However, severe penalties and legal implications make everyone fall in line. On the other hand, India has a clear mandate on both public and private bodies to secure user data along with a prohibition on cross-border flow of data has been introduced under the Digital Personal Data Protection Act, 2023. Minute unauthorized disclosure will also attract penalty. In contrast, Pakistan operates in a legal limbo where there are no legally binding regulations or laws protecting personal information. This fosters an atmosphere in which privacy intrusions are tolerated and widespread surveillance is normalized.²⁰

8. PECA's Surveillance Powers

In order to prevent cybercrimes and protect the integrity of digital communications, the Pakistani Parliament passed the Prevention of Electronic Crimes Act, 2016 (PECA). On closer inspection, however, PECA serves as Pakistan's main legal tool for state monitoring in addition to being a cybercrime statute. The law gives state agencies, especially the Federal Investigation Agency (FIA) and the Pakistan Telecommunication Authority (PTA), extensive and unrestricted surveillance powers, despite having some helpful provisions for thwarting real cyber threats (such as fraud, harassment, and identity theft). With little to no judicial oversight, the government can monitor, intercept, and keep digital communications thanks to the authority granted by Sections 31 to 39.²¹ The surveillance architecture of PECA does not encompass a singular clause; it constitutes a stack: rapid preservation Section 31, bulk retention Section 32, warrants to search and disclosure Section 33 and 34, operational powers Section 35 and 36 platform level takedown Section 37 and real time interception Section 39. In combination, these instruments can allow constant access into the digital lives of the citizens. The legal issue on the

¹⁹ *What Is GDPR? Summary of General Data Protection Regulation* (Securiti.ai, published approximately 2 years ago) <https://securiti.ai/what-is-gdpr/> accessed 4 August 2025.

²⁰ Clodian, *Data Protection Principles: Core Principles of the GDPR* (3 September 2021) <https://cloudian.com/guides/data-protection/data-protection-principles-7-core-principles-of-the-gdpr/> accessed 4 August 2025.

²¹ *Federal Investigation Agency (FIA) of Pakistan* (PakSearch360) <https://paksearch360.com/law-enforcements-in-pakistan/federal-investigation-agency-fia-of-pakistan/> accessed 5 August 2025.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

constitutional level is whether the intensity of such visibility is confined by legality, necessity, and proportionality of Articles 14 (right to privacy/dignity), and Article 19 (freedom of speech).

Section 31 (Expedited preservation and acquisition of data) provided Expedited Preservation under PECA enables an authorized officer to direct preservation of certain electronic material so as to prevent its destruction providing the court with a notice within 24 hours and can be approved by up to 90 days that can be extended. Although it is meant to protect volatile evidence it allows people to spy on each other as information can be frozen without the user being aware that he is being investigated and no instruction is mandated in informing him/her later that data was being spied on. Such secrecy threatens to chill speech (Article 19) and infringe privacy (Article 14) of journalists, activists, and political opponents in particular. In other countries, they have powers but with safeguards of specificity affirmed by strong specificity, the notification on the user occurring after the investigation process, and the independent audit, which are not found in PECA. They are needed because, in their absence, Section 31 may turn into a surveillance device of low exposure that preserves evidence.²²

Section 32 Bulk Retention of traffic data requires all service providers to store the traffic data of the users (metadata) within 1 year, and access to it should be restricted by court warrant (Sections 33 and 34). The metadata may show social networks, habits, and locations which are not pleasant to them. The blanket, targeted retention turns the presumption of privacy on its head and flies against proportionality concerns of both Article 14 civilization and 19 of the freedom of speech and expression, particularly combined with the Web Monitoring System (WMS). Sections 33 and 34 states about Warrant for Search or Seizure and Warrant for disclosure of content data that give the power to the courts to allow restricted search, confiscation and likely disclosure of content data, subject to

²² Government of Pakistan, *The Prevention of Electronic Crimes Act, 2016 (Act No. XL of 2016, 19 August 2016)* (Sindh Judicial Academy) https://sja.gos.pk/assets/Acts_Ordinances_Rules2/PEC2016.pdf accessed 6 August 2025.

Umer Gilani, Haroon Baloch, Shaheera Jalil Al-Basit and Furhan Hussain, *Electronic Data Protection in Pakistan: What Needs to be Done?* (Bytes for All, Pakistan, in collaboration with Association for Progressive Communications and Privacy International, November 2017) https://www.apc.org/sites/default/files/Data_Protection_in_Pakistan.pdf accessed 6 August 2025.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

exceptional aspects of exigency in the face of cyber-terrorist crime. In spite of its face-saving protection of due process, the absence of threshold probable-cause standards, minimization rules, transparency, and post-investigation notice following the investigation complicates the overreach safeguards. Section 35 and 36 Powers of an authorized officer and Dealing with seized data or information system which empower the grant officers to demand the assistance of decryption and manage the process of seized data. Without previous deletion and minimization obligations, confiscated data may be held permanently, which is incompatible with the Article 14 informational self-determination. Section 37 of the Prevention of Electronic Crimes Act, 2016 (PECA) gives the Pakistan Telecommunication Authority (PTA) a wide power to block, remove, or order removal of online content that is considered as unlawful. This is practically an extension to the platform level control of online content by the PTA. First, PECA did not specify any procedural rules relating to this power and the possibility to arbitrarily exercise it was of concern to the judges.²³ In the case of *Awami Workers Party v. Another* decision is PTA case (IHC, Sept. 12, 2019) where the Court found the blocking of the party web site by the PTA, without serving any prior notice or providing an opportunity of being heard, to be a violation of principles of natural justice and Article 10-A (due process) and the Court required the PTA Government to formulate rules under Section 37(2).²⁴ Following repeated criticism, the government/PTA on its part, published elaborate Rules, namely Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules in the year 2020 to establish system of procedures and oversight mechanism to exercise Section 37 powers, yet civil society and legal commentators have persisted in asserting the over breadth of the provision Section 37, the Rules and that they would allow arbitrary/interim platform-level regulation.²⁵ Lastly, practical implementation has featured national

²³ Government of Pakistan, *The Prevention of Electronic Crimes Act, 2016* (Act No XL of 2016, 19 August 2016; published on Sindh Judicial Academy website) https://sja.gos.pk/assets/Acts_Ordinances_Rules2/PEC2016.pdf accessed 7 August 2025.

²⁴ *Awami Workers Party v Pakistan Telecommunication Authority* (Writ Petition No 634 of 2019, Islamabad High Court, judgment delivered 12 September 2019) <https://globalfreedomofexpression.columbia.edu/cases/awami-workers-party-v-pakistan-telecommunication-authority/> accessed 7 August 2025.

²⁵ Government of Pakistan, *Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2020* (S.R.O. 1077(1)/2020, notified 6 October 2020; published in *Gazette of Pakistan*,

Internet surveillance, including web-monitoring systems and automatic filtering or requests over to platforms, something the civil-society sector and news organizations term as continual surveillance or systematic traffic-monitoring to control content. That fact on the ground can be understood as to why commentators assert that Section 37 and the Rules invite platform-level regulation that can have a chilling effect on political speech.²⁶ Section 39 provides Real Time Collection and Recording of Information that enables court-ordered, time-constrained (7 days, extendable) real time interception of traffic data and content. It may be proportional provided one considers it is used narrowly, but without audit procedures, specific selector requirements and reporting on transparency, the measures run the danger of abuse and quasi-permanent surveillance.

9. Comparative Legal Approaches to State Surveillance and Privacy

It is also important in the analysis of how Pakistan has approached its legislation to balance national security interests and the room that it has provided the inherent right of privacy. Many of the cases below demonstrate the ways in which mature democracies have struggled with these tensions in the United States and the United Kingdom so that they can present us with cautionary tales as well as more successful moments of learning.

I. United States: Carpenter Doctrine and Fourth Amendment

The right to privacy under non-consensual surveillance is enshrined in the fourth amendment to the constitution of the United States, to protect against the unreasonable searches and seizures. The extent of jurisprudence has been founded in this provision which dictates how the state can intrude in the intimacies of the citizen life. Police surveillance usually demands a legal warrant backed with probable motivation. This guarantees an essential balance to unwarranted or unwarranted monitoring. The greatest change in this direction came with the *Carpenter v. U.S. Supreme Court* (2018), ruling in the United States. It concerned the process of the

20 October 2020) <https://www.scribd.com/document/484930544/Removal-and-Blocking-of-Unlawful-Online-Content-Procedure-Oversight-and-Safeguards-Rules-2020/> accessed 8 August 2025.

²⁶ *PTA Using Web Monitoring System to Block Online Content in Pakistan, NA Told* (Pakistan Today, 29 August 2024) <https://www.pakistantoday.com.pk/2024/08/29/pta-using-web-monitoring-system-to-block-online-content-in-pakistan-report/> accessed 8 August 2025.

government accessing the historical cell-site location information (CSLI) developed by telecom businesses without taking a warrant. The Court ruled that although CSLI data is in possession of third parties, there is still a justified expectation of privacy in relation to location data by individuals. Hence, retrieving such data without a warrant was against the fourth amendment. The ruling was noteworthy in that it narrowed the “third-party doctrine,” which once supported the government in the gathering of the data communicated to a third party (such as to a phone company or a bank) without a warrant. Besides the constitutional protections, the U.S. has put in place statutory regimes to control surveillance under national security. Foreign powers and agents of foreign powers may be monitored under the Foreign Intelligence Surveillance Act (FISA) under the judicial oversight of the secretive Foreign Intelligence Surveillance Court (FISC). In as much as FISA has been accused of seating in obscurity, it still obligates the government to place its case in front of an independent judicial authority hence factoring in some degree of accountability. After Edward Snowden released information regarding mass surveillance conducted by the National Security Agency (NSA), USA Freedom Act of 2015 was passed. This law reduced the government powers to perform bulk collection of telephone metadata and provided further transparency and authorities to oversee the surveillance procedure. These reforms were an indication of the increasing societal and judicial insistence on the privacy issue under the digital era, even under national security.²⁷

II. United Kingdom: Dual-Lock Surveillance and Investigatory Powers Act

In situating surveillance and privacy, United Kingdom has utilized a legislative approach aimed at finding a nominal balance between efficiency of operation to intelligence services and control over surveillance in the defense of civil liberties. The most notable jewel in the UK big brother surveillance system is the Investigatory Powers Act 2016 which is also referred to as the Snoopers Charter. The Act bestowed significant authority to data collection and interception by intelligence agencies and law enforcement, but established significant safeguards, as well. The dual-lock system of interception warrants is one of the major innovations

²⁷ *Carpenter v United States* (U.S. Supreme Court, No 16-402, decided 22 June 2018) <https://www.oyez.org/cases/2017/16-402> accessed 9 August 2025.

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

of the IPA. In this system, such a warrant has to be authorized by a cabinet minister and also someone senior judge. The combined need assures that the surveillance choices are not taken just in the executive house and creates judicial oversight as a balance to abuse.²⁸ Moreover, a new office of Investigatory Powers Commissioner, introduced by the Act, has a supervisory role, which involves audits and reviewing of the exercise of surveillance powers, so as to maintain its use within the law. This office is established to be independent hence increase institutional checks.²⁹ Nevertheless, the IPA also brings upon it some controversial points, like the necessity of the Internet Service Providers (ISPs) keeping records of internet connections up to a year. This implies that the government will have information on what sites an individual has accessed although this is not presented to the state. The critics hold that this amounts to mass surveillance and can lead to violation of the privacy rights of individuals, unless the privacy is effectively provided with encryption and the use properly restricted.³⁰ Notwithstanding these reservations, the UK approach suggests trying to legalize and formalize surveillance activities by means of detailed regulations and official supervision, as opposed to the discretionary authority under the executive or the informal surveillance attitudes. Judicial review, transparency reports and Parliamentary scrutiny also act to enhance the balance of striking the balance between the security and privacy.³¹

10. The Right to Privacy as a Fundamental Right in India

The surveillance and privacy practices in India have taken a new turn in the recent

²⁸ Shaheed Fatima K.C., "The 'Snooper's Charter' and Judicial Oversight" (Just Security, 21 December 2015) <https://www.justsecurity.org/28443/snoopers-charter-judicial-oversight/> accessed 10 August 2025

Home Office, *Report on the Operation of the Investigatory Powers Act 2016 (Accessible Version)* (statutory report laid before Parliament 9 February 2023) <https://www.gov.uk/government/publications/report-on-the-operation-of-the-investigatory-powers-act-2016/home-office-report-on-the-operation-of-the-investigatory-powers-act-2016-accessible-version> accessed 10 August 2025.

²⁹ Daniella Lock, *The Investigatory Powers Act: The Official Entrenchment of Far-Reaching Surveillance Powers* (Just Security, 30 November 2016) <https://www.justsecurity.org/35040/investigatory-powers-act-official-entrenchment-far-reaching-surveillance-powers/> accessed 10 August 2025.

³⁰ Meredith Broadbent, *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers* (CSIS Audio Brief, 21 May 2024) <https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhances-government-surveillance-powers> accessed 10 August 2025.

³¹ Investigatory Powers Bill, HL Deb (House of Lords), vol 773, col 1359 (27 June 2016) <https://hansard.parliament.uk/lords/2016-06-27/debates/73D5BB49-5EE4-437F-AC1C-BC739515A6A0/InvestigatoryPowersBill> accessed 10 August 2025.

past by mostly taking the form of judicial interpretation. One of these highlights was the ruling of the Supreme Court in the case of *Justice K.S. Puttaswamy v. AIR 2017 SC 4161 Union of India*, which essentially reshaped the face of the law by considering the right to privacy as a fundamental right under the constitution. The Court also believed that the premise of privacy is an inbuilt part of the right to life and the Right to personal liberty, as entrenched under Article 21 of the Indian Constitution. This determination was in the form of overturning previous cases to give privacy a central-level guarantee.³² More importantly, in Puttaswamy decision also formulated a three-fold test any law that allows surveillance to occur must satisfy: (1) legality, such that surveillance can only be sanctioned by a legislative enactment, (2) necessity, that the state must be able to justify its act of surveillance as furthered by a valid aim (national security and public order); and (3) proportionality, where the surveillance measure involved must only interfere with individual rights to the minimum level possible. This framework tries to strike the balance between the state interests and civil liberties and makes the judicial scrutiny the center of any intrusion over the privacy.³³ Side by side with this court trend, India has also been trying to enact fully fledged data protection via the Draft Personal Data Protection Bill (2023). This bill has a lot in common with GDPR of the EU, as it focuses on data processing with the consent, limitation of purposes, and responsibility. It aims at establishing an independent body to oversee Data Protection, and high requirements on the data fiduciaries to include government agencies. Nevertheless, the bill has also received some criticism because it has provided the state with wide exemptions based on the excuse of sovereignty and public order that the bill may undermine privacy protections practically. However, the Indian legal trend of powerful judicial activism and expanding regulatory code hints to an emerging awareness of the necessity of securement of personal information and privacy amidst

³² Joyston D'Souza, *SCO Shorts: Right to Privacy* (Supreme Court Observer, 23 August 2022) <https://www.scobserver.in/journal/sco-shorts-right-to-privacy/> accessed 11 August 2025. Law Blend, *Justice K.S. Puttaswamy vs Union of India: Right to Privacy as a Fundamental Right* (Law Blend, 30 June 2025) <https://lawblend.com/articles/justice-k-s-puttaswamy-vs-union-of-india/> accessed 11 August 2025.

³³ Nidhi Singh, *Defining the Right to Privacy in India in Light of Justice K.S. Puttaswamy & Anr. v Union of India* (2017) (Oxford Human Rights Hub Blog, 5 October 2017) <https://ohrh.law.ox.ac.uk/defining-the-right-to-privacy-in-india-in-light-of-justice-ks-puttaswamy-anr-v-union-of-india-2017> accessed 11 August 2025.

the rising digital surveillance.³⁴

11. GDPR and Digital Rights in the European Union

European Union has since established itself as a trailblazer in the privacy and data protection sector mainly due to their ground breaking legislation- the General Data Protection Regulation (GDPR), which was implemented in 2018. GDPR transforms data processing into a rights-based approach with stringent application of its provisions even on other enterprises outside the EU that process data of EU citizens. In essence, GDPR has a number of principles that have formed the foundation of the regime, among them being the requirement that data needs to be collected with informed consent; its use need to be limited to a specific, lawful purpose (purpose limitation); the right to access, rectify, or erase data (including the so-called right to be forgotten); and supervisory frameworks that require independent control by national data protection authorities. Any violation may invite harsh penalties, hence providing substantive enforcement.³⁵

A significant legislative trend in the regard has been the case of Digital Rights Ireland v. Article 26(1), Minister for Communications (C-293/12). Data Retention Directive (2006/24/EC) required telecom companies to store metadata within a maximum period of two years and was invalidated by the Court of Justice of the European Union (CJEU), as it interfered with all the essential freedoms. The Court held that the order amounted to an unjustifiable interference with the right to respect for private and family life combined with the right to protection of personal data, both which are conferred in the EU Charter of Fundamental Rights. Furthermore, the Court emphasized that the retention of data in general and without differentiation was not democratic and must be kept to a minimum. The case among later cases such as Schrems I and Schrems II signify the willingness of EU to assume the privacy as an embodiment of the statutory rights rather than only as a right. The legal system of the EU therefore constitutes a good example of how democratic societies could enshrine privacy however in providing surveillance and law

³⁴ Nidhi Singh, *The Digital Personal Data Protection Act, 2023: A Constitutional and Regulatory Analysis* (The Amikus Qriae, 2025) <https://theamikusqriae.com/the-digital-personal-data-protection-act-2023-a-constitutional-and-regulatory-analysis/> accessed 11 August 2025.

³⁵ Shobhit Seth, *All You Need to Know About GDPR, the New Data Law* (Investopedia, updated 24 April 2023) <https://www.investopedia.com/investing/all-you-need-know-about-gdpr-new-data-law/> accessed 12 August 2025.

enforcement needs of the state as well.³⁶

12. The Digital Panopticon

The Legal and Philosophical Basis Modern surveillance is best described by the metaphor of the Panopticon which was first put forward by an English philosopher called Jeremy Bentham. The system structuralism by Bentham focused on a prison in which the inmates could be monitored whenever without knowing when they were being spied, thus self-regulating. Later in *Discipline and Punish* (1975), Michel Foucault extended this idea to an observation of how surveillance can be an all-enveloping way of social control in contemporary states. This metaphor is very relevant to the context of Pakistan because of how the act of Prevention of Electronic Crimes Act (PECA), 2016, is structured and implemented. PECA gives extensive and sometimes vaguely defined authority to eleven-investigative outfits such as the FIA and puts little restrictions on judicial authorization or control. This leads to the creation of an electronic Panopticon in which the citizen-subjects live in the threat of being watched at any one time- through social media use, email, phone records, or online messages.

In the case of this kind of surveillance, it is not necessarily transparent, but its existence can be sensed, and people change their ways to avoid criticism, terminate criticism, and act by censoring themselves. The possibility of being monitored, even without a real monitoring, is enough to change the democratic participation. This structural imbalance is further exacerbated by the opaqueness of the state surveillance mechanisms, whereby the party that conducts surveillance is neither clear nor answerable. In such a system the constitutions values rest under serious threats. Freedom of speech guaranteed by Article 19 and the right to a fair trial specified in Article 10A are impaired under these facts when citizens are not free to express their backs or have no confidence that the digital evidence gathering against them will be based on a legitimate hard-earned basis. In addition, judicial checks or legislative oversight on the progress with PECA, results in the fact that

³⁶ Kenneth Propp and Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision* (Lawfare, 17 July 2020) <https://www.lawfaremedia.org/article/geopolitical-implications-european-courts-schrems-ii-decision> accessed 12 August 2025.

the system of surveillance is placed in the legal vacuum without any attachments to democratic checks and balances. Metaphor of Panopticon is therefore not just an hypothetical one- it is a living reality to the digital citizenry in Pakistan. A change in the legal design, which enables such spying, is also crucial to achieve a more just and democratic society whereas clearly the principles of legality, necessity, and proportionality should be factored into it, as it is evident in the comparative models, which are considered above.³⁷

13. Policies and Law Changes

The prevailing legal and institutional framework of control over surveillance in the environment of the Prevention of Electronic Crimes Act (PECA) is hardly capable of managing with the mounting dangers to personal privacy and of democratic liberties in the digital era of Pakistan. With no concrete data protection statutes, judicial check, or a clear system of accountability being in place, the lack of a robust framework has resulted in a legal void that undermines rights of the individual and constitutional protections as the powers of state surveillance agents to search legal mandates remain vaguely defined. Based on international standards of practice and comparisons, this section proposes the organizational changes and policy-based incisions that Pakistan will need to implement in order to correct its surveillance apparatus to its constitutional and international commitments.³⁸

14. Passing of a General Data Protection Law

The most basic measure that can be undertaken towards safeguarding digital privacy in Pakistan is the passage of an effective and comprehensive law on data protection. Currently, there is no single legislation, which can regulate the manner in which personal data is gathered, stored, processed, or shared by both the public and the private sector. The current arrangements of PECA and sectoral laws are diffuse,

³⁷ Qazi Mohammad Shayan, *The Panopticon Reimagined in the Age of AI and Digital Surveillance* (Pakistan National CERT, CyberTech Chronicles blog) <https://pkcert.gov.pk/blog/the-panopticon-reimagined-in-the-age-of-ai-and-digital-surveillance.asp> accessed 13 August 2025.

Fatima Raza, *A Panopticon Society?* (The Express Tribune, 16 September 2024) <https://tribune.com.pk/story/2496505/a-panopticon-society> accessed 13 August 2025.

³⁸ r/Intelligence, *"The surveillance system keeping tabs on millions"* (Reddit, 4 January 2013) https://www.reddit.com/r/Intelligence/comments/1du00tv/the_surveillance_system_keeping_tabs_on_millions/ accessed 13 August 2025.

Josh and Mak International, *Data Protection in Pakistan* (Josh and Mak International, 2023) <https://joshandmakinternational.com/data-protection-in-pakistan/> accessed 13 August 2025.

their scope is minimal, and they do not provide meaningful protection to the individuals.³⁹ A Personal Data Protection Act should be worked out which should be applicable to both state material and to the individual organizations. The legal framework should clarify the range of data to be considered under the terms of personal data and sensitive personal data and consent so that the ambiguity is not turned into the loophole of illegal processing of the data.

In addition, the laws should have an independent Data Protection Authority (DPA), which is charged with compliance monitoring and initiatives and unlawful cases examination and fine bringing up where viable. This body must not be under the executive control and must be backed by the courts in a way its effect is binding and unbiased in decisions. Notably, individuals should be given a degree of enforceable rights under the law, among them, the right to access their personal information, correction, erasure (where possible), and the objection to misuse. A judicial redress mechanism should also be put in place to pursue remedies and compensation in the event victims suffer breaches of data or misuse of surveillance. The Indian Digital Personal Data Protection Act (2023) and the European Union general data protection regulation (GDPR) provide the best models, particularly in the way they deal with treatment of consent, purpose limitation and enforcement framework. The absence of a similar law will continue to expose Pakistani people to the exploitation of the corporations as well as uncontrolled influence of the government and state.⁴⁰

15. Establishment of Control Organization

The formation of an independent oversight body that would specifically exist to monitor any type of state watching has been one of the most urgent institutional changes that should happen. At the moment, the surveillance practices in Pakistan take place under little oversight with the law enforcement agencies having absolute

³⁹ Saifullah Khan and Saeed Hasan Khan, *Data Protection & Privacy 2025 – Pakistan* (Chambers and Partners, 11 March 2025) <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2025/pakistan> accessed 13 August 2025.

⁴⁰ Yousaf Amanat & Associates, *Comparing PECA 2016 and the Personal Data Protection Bill 2023: A Critical Analysis of Cybercrime and Data Privacy Laws in Pakistan* (Legal 500, 29 April 2025) <https://www.legal500.com/developments/thought-leadership/comparing-peca-2016-and-the-personal-data-protection-bill-2023-a-critical-analysis-of-cybercrime-and-data-privacy-laws-in-pakistan/> accessed 13 August 2025.

power. This institutional unreliability cultivates the systemic abuse and compromises trust of the people. Authority of the proposed oversight body must be directly to Parliament and not to the executive in a bid to assure democratic legitimacy and institutional independence. The essence of its core functions must entail post-surveillance judicial oversight, data access request auditing, handling of compliance statutory limitation, and the effects of surveillance on civil liberties. The body must be empowered to call officials to order, request records and punish illegal acts by the state agents. Moreover, it must be given the authority to accept and answer the allegation of illegal surveillance made by any individuals who fear that they are under on illegal surveillance. The oversight body will also be required to publish annual transparency reports and impact assessments that should lead to the development of a culture of transparency and deterrence against abuse by establishing a public record of the use of surveillance. In absence of such institution, the activities of surveillance are going to be conducted under secrecy building breeding ground of offending the constitution.⁴¹

16. Legal Recognition of Privacy as a Fundamental Right

Despite the clause 14 of Pakistan Constitution that gives the concept of dignity of man and privacy of home, the issue of informational privacy i.e., the right to control own personal information and digital footprint has not found any constitutional jurisprudence. This silence has enabled the courts to take avoidance of discussing the issue of surveillance breaches and it has left the citizens without any legal grounds to oppose such practices that result in abuse of data. As a measure to remedy this, the judiciary and the Parliament should acknowledge privacy as a stand-alone fundamental right, which is closely related to the right of liberty, dignity, and autonomy. The Supreme Court must borrow the meaning methodology employed by India in the Puttaswamy case which relied upon the right to privacy contained in Article 21 of the Indian Constitution. This case established a three-fold test of

⁴¹ Hija Kamran, *Between Privacy and Power: The Fine Line in Pakistan's Data Protection Bill* (GenderIT, 5 March 2025) <https://genderit.org/articles/between-privacy-and-power-fine-line-pakistans-data-protection-bill> accessed 13 August 2025.

Oves Anwar, *Cyber Surveillance and Big Data: Pakistan's Legal Framework and the Need for Safeguards* (Research Society of International Law, 2023) <https://rsilpak.org/wp-content/uploads/2023/03/CYBER-SURVEILLANCE-AND-BIG-DATA-PAKISTANS-LEGAL-FRAMEWORK-AND-THE-NEED-FOR-SAFEGUARDS.pdf> accessed 13 August 2025.

legality, necessity and proportionality, stipulating any violation of privacy must be justified by law, including a genuine state need, and be the least inconsiderate indeed the test, to put it in other words, compels a violation of privacy to fulfill a lawful requirement, demonstrate a legitimate demand of the state, and be the minimal intrusive facility. This kind of doctrinal establishment would not only generate judicial discipline of surveillance cases but will also influence subsequent codification since all laws that affect privacy will be of high benchmark in the constitutions. An explicit acceptance of privacy would also enhance higher compliance of Pakistan with international standards of human rights, including the ICCPR, and set up a more citizen-oriented government under the digital world.⁴²

17. Recommendations

The best way to change the current state of affairs in Pakistan is to introduce the digital surveillance environment to a multi-stakeholder view that would help to preserve the right of every individual to privacy enshrined in the Constitution and laws. Legislative stasis, silence on the part of the courts and ignorance on the part of the general citizenry have each been contributing factors with regard to such a system in which the state is disproportionately empowered, and individuals made vulnerable. Based on these findings, the recommendations below provide clear steps which should be taken collectively by the legislature, judiciary and civil society to work towards rebuilding the trust and make sure that the digital ecosystem is conforming to the constitution and a rights-based ecosystem.

Legislature

The extensive role of Parliament would be the responsibility of designing an architecture of laws that could facilitate national security as well as safeguarding the rights of individuals. The immediate aspect is that the lawmaking body should enact an effective Personal Data Protection Bill without delay and make sure that it has the main protective provisions, as in EU GDPR as well as the Indian Supreme Court judgment *Puttaswamy*. These are informed consent, purpose limitation, transparency, binding individual rights, and high accountability of both the public

⁴² Doon Law Mentor, *Right to Privacy Under Article 21: Challenges in the Digital Age* (Doon Law Mentor, 4 April 2025) <https://doonlawmentor.com/right-to-privacy-under-article-21-challenges-in-the-digital-age-2025/> accessed 13 August 2025.

and the private data controllers. Additionally, an action should be taken in amending the Prevention of Electronic Crimes Act (PECA). The part of monitoring, in particular, Sections 29-34, need to be amended considerably. Effective framework to judge and review should be established against any arbitrary interception or access to any private communication. Surveillance orders must be time limited, must have sunset clauses and processes of destruction of data. More importantly, the legislation should have clear mechanisms of remedies against those, whose rights are being violated either by unlawful surveillance, misconduct of data, or unlawful removal of content. Lastly, the Parliament ought to establish a Privacy Commission with investigatory, adjudicatory and regulatory powers. This body should be capable of enforcing norms of data protection, inquire into complaints of abuse of surveillance, and supervise execution of PECA. Needless to say, its autonomy over the executive branch will be paramount in maintaining impartiality and confidence in its work.

18. Judiciary

Privacy should no longer be viewed as a secondary or peripheral right by the courts of law especially the Supreme Court. The judiciary is highly required to come up with a binding jurisprudence that clearly establishes the right to informational privacy as a fundamental right under Article 14 of the Constitution and one that is implicit in the human dignity and personal liberty. Considering the precedent of the Puttaswamy case in India, the court ought to establish a constitutional test of the rights that are violated in the digital realm, resting on the legality, necessity and proportionality principles. Any data collection practice or even surveillance regime should be evaluated in terms of this three-part standard. Through this analysis, the judicial system will be able to evaluate state actions in a systematic way and give directions to future legislation that is constitutional in nature. Furthermore, it is the duty of the judiciary to act in a paternalistic role overpower against vulnerable populations, who are most often targeted by surveillance especially whistle blowers, investigative journalists, and civil society activists. Courts ought to protect such actors through public interest litigation or *sou motu* to prevent the surveillance, which is either revengeful or political in nature and in the process assure democratic participation and accountability.

19. For Civil Society

A civil society organization is required in critical roles to influence the tone of the discussion in the society, criteria and institutional reforms, and monitor power to levels of accountability. Among the most direct and influential contributions is the one that introduces awareness building activities around the country regarding digital rights, the threat of surveillance, and the preservation of privacy. Education can be one of the most effective modes of empowerment in the society where most users remain ignorant of the data collection and misuse channels. Besides advocating, the civil society should document and litigate abuse mistakes related to surveillance. This involves developing a record of illegal interception, over-broad removal of content, or data abuse by governments. High courts and the Supreme Court have a chance of setting precedes that will turn down excessive surveillance via strategic litigation. Finally, the civil society must always work to ensure more visibility and responsibility in the PECA implementation processes. This entails a requirement that Parliament carry out regular audits and disclosures of surveillance activity as well as having enforcement agencies release yearly transparency reports about the intelligence they seek, the level of data access or interception, and how frequently they do so. Such practices will take surveillance activities out of the gloom and into the purview of democratic oversight.

20. Conclusion

Unregulated growth of digital surveillance in Pakistan has rendered the right to the privacy practically nullified as a result of the legal and social circumstances in that country. Although constitutional provisions suggest safeguarding personal dignity and privacy of life, the existing laws do not cover the individuals against arbitrary and excessive state invading. More specifically, the Prevention of Electronic Crimes Act (PECA) allows broad surveillance authorities, not subject to judicial oversight or other time constraints, or practical accountability. This is worsened by the inability to implement a strong data protection law that would protect personal data against misuse by government and other individuals. It is in this vacuum that surveillance architecture appears more and more like the digital Panopticon, where one is never sure that one is being monitored but adjusts his or her behavior on the theory that he or she is. This poses dire consequences not only to the freedom of an individual,

Online ISSN

3007-3197

Print ISSN

3007-3189

<http://amresearchreview.com/index.php/Journal/about>

but also to democratic involvement, freedom of speech, and the very well being of the constitutional framework of Pakistan as a whole. Legal reform should be multifaceted to go against this direction. It is high time that parliament enacted a sound data protection legislation and changes to PECA that inject aspects of judicial oversight, limiting the purposes and redress. The court should come to the fore and establish the right to informational privacy as a constitutional right in addition being a civil society and demanding transparency and accountability of the legislator and the enforcers. It is only by coordinated action across these areas that Pakistan can develop a legal framework that ensures the dignity of its citizens and does not accede to normalization of surveillance.