



DIGITAL SURVEILLANCE AND THE RIGHT TO PRIVACY IN PAKISTAN: A LEGAL AND CONSTITUTIONAL ANALYSIS

Muhammad Nauman Sabri

*LLM Scholar, College of Law, Government College University Faisalabad,
Email: advocatenaumansabri@gmail.com*

Muhammad Shaharyar Sabiri (Corresponding author)

*Lecturer, Department of English Language and Literature, The University of
Faisalabad,*

Email: Shaharyarsabiri.eng@tuf.edu.pk

Abstract

Right to privacy is identified as a human right that needs to be protected. This research was aimed to explore the ways in which constitutional framework of Pakistan defines and safeguards the right to privacy in this digital era. Moreover, the study also evaluated the degree to which existing Pakistani laws on digital surveillance aligned with constitutional provisions of privacy. In addition to this, the study also analysed the ways in which linguistic constructions in legal and policy texts influenced the legal understanding and justification of the right to privacy. The study used a mixed-method approach as both doctrinal legal analysis and Critical Discourse Analysis (CDA) was used by the researchers. Moreover, the researchers assessed constitutional provisions, statutes, judicial decisions along with national cybersecurity policies. The findings of the study revealed that the constitution recognised privacy, but this was also undermined by its own conditional phrasing and same was observed with other documents that were used for the analysis. In addition to this, it was also found that the linguistic framework of all these policy documents collectively constructs an ideology. This study played a vital role in studying law as well as overall discussion of digital rights and governance within Pakistan

Introduction

The digital era has converged surveillance and privacy as one of the toughest legal and constitutional issues facing Pakistan. Right to privacy is identified as a human right and is guaranteed under Article 14 of the Constitution of Pakistan, but it faces a threat in the growing surveillance apparatuses of the state and ineffective data protection frameworks. (Daudpota, 2016). As the world becomes a fast-paced digitalized system in terms of governance issues, communication, and life administration in general, the legal sphere in Pakistan has been unable to strike a balance between personal privacy and the demands of national security. (Abbas et al., 2023). Moreover, constitutional jurisprudence in Pakistan was influenced by Islamic ideology that held the view that privacy is highly privileged, as portrayed in Quranic prohibitions towards spying and unjustified access to individual areas. (Hayat, 2007). However, the clear boundaries of privacy rights in their real-life application have been impaired by the ambiguous legal definitions of privacy and the growing trend of the use of digital surveillance by the state itself. The introduction of the Prevention of Electronic Crimes Act (PECA) 2016 (Yongmei & Afzal, 2023) have further fuelled the discussion on whether state control and digital freedom enjoyed by citizens are permissible or a threat to the sovereignty of nations, and critics believe that the laws legitimise excessive surveillance and restrain civil liberties (Shah & Butt, 2025).

Moreover, past literature also mentioned that the Investigation for Fair Trial Act, 2013, aimed at regulating the surveillance by the oversight of a court and its protection against



privacy infringement are slack and subject to misuse (Daudpota, 2016). Furthermore, the new framework of digital colonialism emphasises the impact of external forces and international standards of data on the policies of surveillance and data governance in Pakistan (Ali, 2025). Such an association of international and national factors has resulted in the complexity of the legal nature, where protecting privacy is nothing compared to state interests. Recent literature highlights the importance of the adoption of a comprehensive law on data protection in Pakistan in accordance with the international human rights new requirements and enhancing the protection of the individual against online incursion (A. J. Khan et al., 2025). The comparison with Malaysia shows that the continual change of the socio-legal environment needs reforms to maintain privacy without undermining national security (Nisar & Asghar, 2025). On top of that, linguistic framing in legal and policy documents, like the portrayal of surveillance as being needed to ensure national security, serves a central influence in how people and the courts view a citizen's rights to privacy (Jabeen, 2021).

Furthermore, this study critically discussed constitutional and legal processes in Pakistan in control of privacy, their relationship with the international standards and involved use of linguistic constructions in surveillance language as a resource to analyse the legal legitimacy of privacy in Pakistan. In addition to this, the study also aimed to contribute to understanding how digital surveillance is confronting the constitutional declaration of human decency and the inviolability of individual privacy.

Research Objectives

1. To examine how Pakistan's constitutional framework defines and safeguards the right to privacy in the context of digital surveillance.
2. To evaluate the extent to which existing Pakistani laws on digital surveillance align with constitutional protections of privacy and human rights obligations.
3. To analyse how linguistic constructions in Pakistan's surveillance-related legal and policy texts influence the legal understanding and justification of the right to privacy.

Research Questions

1. How does Pakistan's constitutional framework define and protect the right to privacy in relation to digital surveillance?
2. To what extent do existing Pakistani laws on digital surveillance comply with constitutional guarantees of privacy and human rights standards?
3. How do linguistic constructions within Pakistan's surveillance-related legal and policy texts shape the legal understanding and justification of the right to privacy?

Significance of the study

This research is important to the study of law as well as to the overall discussion of digital rights and governance within Pakistan. Through critical analysis of the provisions of the constitutional and statutory frameworks in Pakistan regarding the rights to privacy in the digital era of surveillance, the study will add a better insight into the contents and constraints of the rights to privacy as per the national and international laws. On the doctrinal level, the research offers a wide legal discourse to analyse the constitutional issues, laws and judicial interpretations which determine privacy protection in Pakistan. This is more so because the high rate of technological advances has exceeded the pace of privacy jurisprudence advancements, and therefore, there is uncertainty in striking the balance between individual and state security interests. In addition to this, on the policy level, the research critically analyses whether or not the laws governing surveillance within the country are in line with



constitutional provisions in Pakistan and the International Declaration of Human Rights. It is anticipated that the findings will be employed to inform legal reform and law-making in the digital realm, as well as rights-based governance. Besides this, there is another interdisciplinary relevance, as this study used Critical Discourse Analysis (CDA) to investigate how surveillance practices were constructed and legitimised by legal and policy language. This language aspect enriched the insight into the functioning of power in law and accentuates the insidious aspects of the reinforcement or violation of privacy rights by the use of language. Finally, the research is aimed at contributing to the academic, judicial, and legislative ways of valuing privacy as a constitutional right, and to enhance a clearer, rights-based practice of digital surveillance in Pakistan.

Literature Review

The Right to Privacy: Constitutional and Theoretical Foundations

The right to privacy is universally recognised as an essential fundamental human right, encompassing a wide range of protections necessary for individual autonomy and dignity (Humble, 2021). Theoretically, the concept is a multidisciplinary domain, drawing foundational concepts from law, philosophy, and sociology, making its precise definition complex and subject to cultural variations. (Newell, 1995). Its historical legal roots famously established it as the "right to be let alone", an individual's natural need to be free from unwarranted intrusion and control. Philosophically, the right to privacy is inextricably linked to the dignity of man, protecting personal intimacies, family life, and individual choices, and serving as a basic block of an ordered and decent society. (Schoeman, 1984). At the international level, the right to privacy gained widespread recognition after World War II, being firmly enshrined in human rights instruments. Furthermore, article 17 of the International Covenant on Civil and Political Rights (ICCPR) prohibits arbitrary or unlawful interference with an individual's privacy, family, home, or correspondence, imposing obligations on signatory states to uphold this right. (Praditama & Ranawijaya, 2023). Domestically, constitutional jurisprudence has generally evolved to protect privacy as an inherent aspect of the right to life and personal liberty. In Pakistan, Article 14(1) of the 1973 Constitution declares the "dignity of man and... the privacy of home, shall be inviolable". Judicial interpretation has broadened this constitutional protection far beyond the physical home to include public spaces and all areas where a person maintains a reasonable expectation of privacy.

Despite its constitutional grounding, the right to privacy is not absolute and is generally subject to law and principles of necessary limitation. (Kamenskii, 2024). This reconciliation is managed through the principle of proportionality, which dictates that any state interference must be lawful, necessary, and proportionate to the legitimate aim pursued. However, the advent of the digital era, marked by mass surveillance and algorithmic monitoring, has posed critical new challenges to these traditional foundations, creating a significant tension between personal privacy and the demands of national security. (Verhelst et al., 2020). This technological surge has outpaced the existing legal framework, demanding the urgent introduction of comprehensive, standalone data protection legislation to safeguard individual autonomy effectively in the modern digital age.

Digital Surveillance and Legal Regulation in Pakistan

In the current digital era, privacy and digital surveillance have become the most urgent legal and constitutional challenges in the country. Moreover, Article 14 of the Constitution ensured the right of privacy, but it has become endangered due to growing surveillance and inefficient



legal ways to protect the data (Nandy, 2023). The local legal community has always had problems finding the balance between assuring the individual's privacy and ensuring the national, urgent security needs of the state. This disproportion is an international tendency, and cybercrimes just tend to increase, partially because of a lack of legislation on data privacy and protection in countries like Pakistan (Nabeel & Iqbal, 2025). The legislation of surveillance is framed by two important legislative instruments, namely the Prevention of Electronic Crimes Act (PECA) 2016 and the Investigation for Fair Trial Act (IFTA) 2013. PECA 2016, specifically, has created a lot of controversy as critics state that its ambiguously given clauses condone the practices of over-surveillance, silence of dissent and eventual suppression of civil rights in the name of national security (S. Khan et al., 2019). Although the modern digital dangers are considered in this Act, such as cyber-harassment and illegal access to data, it is too broadly applied so that the government is able to follow modern online activity and criminalise those who do not agree. Also, the IFTA 2013, which was meant to govern surveillance by and of the court, are criticised in the literature as IFTA 2013 being lax and prone to being misused. The proposition of the aspects of linguistic framing by the state in its legal and policy texts tends to create a sense of surveillance as a need for security, which in turn creates an influence over how the judicial system and people in general view the right of privacy of the citizen. (Barnard-Wills, 2013). Additionally, there is also the problem of the framework of digital colonialism, raising concerns about the influence of external forces and international data standards on the domestic surveillance and data governance policies in Pakistan. Such a correlation of facts has led to a complicated juridical situation in which the protection of privacy is usually secondary to state security concerns. (Qamar, 2019). Because the growth and advancement in technology is always above the pace of jurisprudence governing privacy in Pakistan, the trend in literature has remained consistent to signify that Pakistan requires a fully-fledged, ultra-modern data protection legislation to keep up to the level of international human rights demands. (Sabri & Sabiri, 2023).

International Human Rights Standards on Privacy and Surveillance

The basic right to privacy is widely accepted as one of the pillars of human dignity, secured by the basic international documents, and today, debated more than ever in the context of new realities in the digital world. (Humble, 2021). In essence, the international legal doctrine dictates that the surveillance practices should be balanced towards the virtues of legality, necessity and proportionality, which is frequently restated in modern human rights jurisprudence. (Chaara et al., 2022). The same rights are given by this framework to the digital setting as in the real world, by claiming that individuals have the natural right to privacy, whether they are in a physical or virtual location. The right to privacy is not merely an individual guarantee fixed, but is also placed as a fundamental right and as a precursor to other crucial civil and political rights, such as that of freedom of expression and association. (Lever, 2006). In a development attributed to surveillance, especially in the intersection of counter-terrorism and national security, the literature has defined surveillance as a growing danger, as well as a colossal infringement of these rights. This has led to an accelerated rise and development of the privacy debate towards the summit of agendas of international human rights mechanisms, such as the United Nations. (Nandy, 2023).

An important field of academic concern is the legal criterion of reasonable state surveillance. To be authorizable, any measure must first be authorised by explicit, official law (legality), possess a provable, least-invasive means of attaining a valid goal (necessity), and be



such that the extent of intrusion does not exceed the gain to society (proportionality in a narrower sense) (Rønn & Lippert-Rasmussen, 2020). Nonetheless, the development of such powerful means as Facial Recognition Technology (FRT) and mass surveillance threatens this pattern, raising questions on accountability and transparency because of the systematic accumulation of massive personal information volumes. Moreover, the awareness of the presence of ubiquitous digital surveillance leaves a substantial risk, creating a sense of anxiety and distrust and contributing to self-censorship and freezing the discourse democracy as a response (Büchi et al., 2022). This is of critical concern to this scholarly consensus that states should balance domestic surveillance activities with these high international standards to avoid individual rights being compromised in the name of security.

Linguistic Constructions of Law, Power, and Privacy

Critical legal studies are much concerned with the linguistic construction of law, power and privacy, which has mainly relied on Critical Discourse Analysis (CDA) to deconstruct how judicial and legislative language is used to construct and legitimise power within the state. (Mullet, 2018). Moreover, legal discourse is not a neutral rule system; it is an active process of the social construction of reality, in which linguistic decisions perform the active rationalisation of state actions, in which linguistic choices have a leading role in the digital surveillance and counter-terrorism domain. (Riner, 2018). Furthermore, the CDA approach is applied in an academic setting, the aim of which is the establishment of how institutional cognition, as well as underlying ideologies, informs the language of a legal text. (N. L. Fairclough, 1985). One of the main highlighted features is the linguistic strategic framing in which intrusion into the right to privacy is justified. Words like national security, legitimate aims, and public interest are some of the discursive tools which make surveillance seem normal in terms of being an inevitable and reasonable response to existential threats.

This linguistic touch predetermines a power imbalance in which individual privacy tends to be pushed to the background and presented as a subordinate value, which requires a utilitarian approach to collective security. (McDonald & Forte, 2021). The resultant text of the law may be defined by semantic ambivalence and vagueness, among other things, imposing on law enforcement vast formal and informal authority to deploy technologies such as AI in policing without explicit responsibility. Moreover, language AI ethics debates, which introduce misleading rhetoric, such as responsible AI, have been criticised as potentially playing an instrumental role, aiming to present commitment to principles when letting actors off the hook regarding breach of privacy. (Selvam & González Vallejo, 2025). Conclusively, this literature demonstrates that the language of the law is what establishes a power relationship that controls the consent of the people and normalises normal surveillance in the digital era.

The literature available on the issue of digital surveillance and privacy in Pakistan is a great source of information on the aspects of the constitution, statutory growth and the global human rights imperatives, but there is also a significant research gap identified in comparison to the study purpose. Even though it has already been investigated in previous studies what Article 14 of the Constitution refers to and the analysis of the legislation is carried out, including PECA 2016 or IFTA 2013, they do not fully examine how these laws are compliant with the constitutional guarantees and human rights criteria. Furthermore, another under-researched dimension is associated with the language of constitutional and policy documents with respect to the role of linguistic constructions. Previous research is very light on the role of state discourse and law-making language to inform the legal rationale and perception of



surveillance activities, thus making legal infiltration of privacy acceptable. As a result, a research gap can be identified concerning the possibility of combining the doctrinal legal analysis and critical discourse analysis to comprehend the interactions of law, language, and power to determine the concept of the right to privacy and regulate it within the digital governance context of Pakistan.

Research Methodology

The study adopted mixed mixed-method design. (Gay et al., 2008) Both qualitative and quantitative data were used by combining doctrinal legal analysis with critical discourse analysis (CDA). Moreover, it is an exploratory and analytical design aimed at understanding the ways the legal system in Pakistan understands the right to privacy and safeguards it within the framework of digital surveillance. The doctrinal component offered interpretation and assessment of law, whereas CDA made the legal and policy language visible through an interdisciplinary lens to demonstrate the practices of surveillance construction and legitimisation. (Bhat, 2020). The dual approach of the research was significant as the doctrinal analysis examined Constitutional provisions from my legislation and judicial reasonings to assess the protection of privacy within the constitutional framework of Pakistan. Moreover, the CDA component integrated Fairclough's three-dimensional model. (N. Fairclough, 2013) along with van Dijk's socio-cognitive approach (Van Dijk, 1993) This allowed the analysis at the textual, discursive, and social level and also emphasised the cognitive and ideological mechanisms that upheld legal narratives. Moreover, these models also exposed the way institutional discourse normalised surveillance and shaped the legal understanding of privacy.

Data Collection

The study was based on primary legal and policy documents, which included the Constitution of Pakistan, The Prevention of Electronic Crimes Act 2016, The Pakistan Telecommunication Act 1996, the Investigation for Fair Trial Act 2013 and key judgments from superior courts that interpreted privacy and surveillance were also made part of the research. These were made part of the research as the aim of the study was to understand the laws and how they are shaping the views towards digital surveillance and privacy in Pakistan. These collections of policy and legal documents allowed us to understand the discourse at a broader level and also allowed us to analyse these laws in a current modern perspective where technology has evolved beyond imagination. The constitutional provisions, statutes and judgments that either directly deal with surveillance or privacy are given precedence. It extends to include policy texts and government communications in order to capture or reflect the larger discourse in relation to digital governance. The materials used to enhance transparency and reproducibility are based on publicly available materials only.

Theoretic Framework

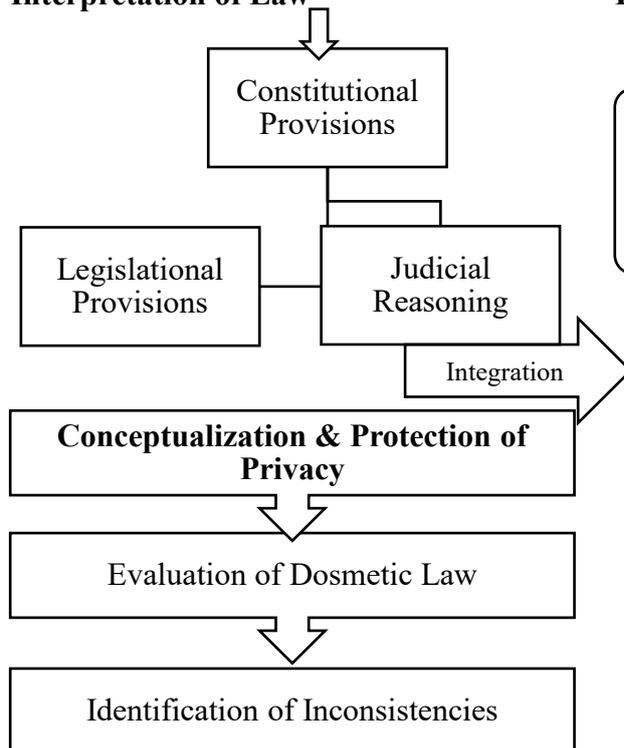
The theoretical framework was designed by the combination of doctrinal legal interpretation and Fairclough-van Dijk CDA model (Bhat, 2020; N. Fairclough, 2013; Van Dijk, 1993). The doctrinal analysis examined the constitutional meaning, statutory intent and judicial rationale to ascertain the extent and safeguard of privacy rights. CDA focused on linguistic attributes, including modality, vocabulary and framing that created surveillance as a requirement, right or even an eventuality. Moreover, the textual, discursive, and social analysis levels by Fairclough showed the ways legal texts interacted with power structures and the socio-cognitive approach by van Dijk elaborated the legal discourse with respect to the influence of ideologies and



institutional cognition. This unified system revealed the overlap between language, power and legal authority within the system of surveillance in Pakistan.

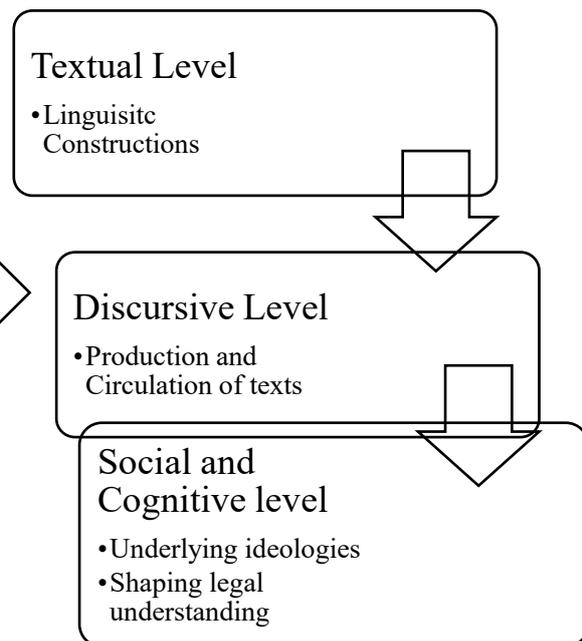
Layer 1: Doctrinal Legal Analysis

Interpretation of Law



Layer 2: Critical Discourse Analysis

Fairclough-Van Dijk Discourse Model



Data Analysis and Interpretation

The data was in a line through close reading and interpretative synthesis as legal provisions and judgments were examined to the textual and proposed interpretation. (Eppley, 2019; Hunter, 2016). In addition to this, CDA identified the linguistic and discursive patterns that either rationalised surveillance or marginalised privacy. Moreover, findings from both analyses were integrated to assess the consistency between Pakistan’s legal discourse and its constitutional and international commitments to privacy. Similarly, the reliability of the research was ensured by the selection criteria and consistent analytical procedures. (Ludovico et al., 2022). Moreover, the validity was strengthened through triangulation between doctrine analysis, discourse interpretation and legal standards. (Golafshani, 2015). The study used only publicly available materials to maintain academic integrity and ethical compliance through accurate citations and critical engagements with the resources.

Results and Discussion

The Right to Privacy in the Context of Digital Surveillance

The constitutional concept of privacy in Pakistan is embedded in Article 14(1) of the Constitution, which states that "the dignity of man and, subject to law, the privacy of home shall be inviolable." This places dignity and privacy at the heart of the constitutional order, yet the clause "subject to law" immediately qualifies its reach. This conditionalizing has enabled



the legislative and executive powers to violate privacy by legalising the same. The privacy, in effect, is not a sanctum, but it is a bargaining given the government's definition of necessity and security. This has produced a jurisprudential tension between individual liberty and collective security. As it has been discovered, the theoretical privilege of privacy has always been recognised by the courts, but it has been hard to implement this protection in checking against surveillance. In *Benazir Bhutto v. Federation of Pakistan* (PLD 1988 SC 416), the Supreme Court linked privacy to personal liberty, holding that "the dignity of the individual is the essence of constitutional democracy." This depicts the redefining of the constitutional ideals on executive necessity.

This has been complicated by the increasing capacity of the state in the conditions of digital surveillance, which has aggravated the constitutional landscape. The absence of explicit constitutional references for informational and online privacy leaves the citizen vulnerable to invasiveness under the laws that were created to control cybercrimes and enhance national security. The impossibility of explicitly protecting the data provisions explicitly in the constitution allowed the state to take into account the privacy within the greater order of provision of security. This dynamic transforms the constitutional guarantee into a flexible instrument of control, which is sustained by the linguistic uncertainty of "subject to law." Moreover, the judiciary considered privacy a principle but scarcely enforced practical restrictions on the executive surveillance. It is a constitutional framework which brings recognition without resilience.

Alignment of Existing Pakistani Laws with Constitutional Protections

The legislative framework in Pakistan demonstrates evident change from privacy protection towards surveillance facilitation. The Prevention of Electronic Crimes Act 2016 (PECA), which is purportedly targeted at combating cybercrimes, has wide-ranging aspects to enable the state agencies to access, monitor, and store user data. Section 29 authorises service providers to retain traffic data "for a minimum period of one year or any period as may be prescribed," while Section 32 empowers investigation officers to "require any person to provide data in his possession." These clauses are not accompanied by strong judicial oversight, and therefore, this permits the administrative bodies to gather and store their personal information at their will. PECA is not consistent with the spirit of privacy in Article 14 in terms of the lack of proportionality and necessity tests.

The Pakistan Telecommunication (Re-organisation) Act 1996 reinforces this pattern by permitting interception "in the interest of national security or public order." The wording here reflects the constitutional limited clause, and copies its ambiguity and broadens the area of legal interference. The Act does not mandate that the interception must be previously authorised by the court of law, but the executive agencies have internal approvals. This absence of external accountability undermines the constitutional promise that privacy may be restricted only "in accordance with law" that is fair, just, and reasonable. The Investigation for Fair Trial Act 2013 (IFTA) was introduced as a corrective measure, the aim of which was the surveillance of judicial warrants. The enforcement has, however, resulted in very little executive power restraint. Under Section 5, intelligence agencies may apply in secret to seek warrant to intercept. The Act defines "surveillance" and "interception" in expansive terms, covering "any electronic, oral or written communication." In theory, this creates a legal pathway for control, but practically, it institutionalises secrecy. The necessities of judicial approval are made



procedural as opposed to substantive, as the reviewing judge relies solely on ex parte details as presented by the intelligence officers.

Case law has continued to enhance this imbalance. In *Mustafa Impex v. Government of Pakistan* (PLD 2016 SC 808), the Court reaffirmed that executive authority must operate within constitutional bounds but did not extend this principle to the domain of electronic surveillance. Similarly, in *Benazir Bhutto's case*, the Court condemned arbitrary intrusion. However, the phrase "subject to law" has become a bridge that merges this contradiction by converting legislative leniency into constitutional compliance. The consistency of the existing Pakistani laws with the constitutional protections is more rhetorical than real. This legal framework produced an illusion of balance while favouring the entitlement of the state over the rights of citizens.

Table 1: Constitutional and Legislative Framework

Instrument	Key Provisions Related to Privacy	Mechanisms Enabling Surveillance	Degree of Alignment with Article 14 (Privacy and Dignity)	Analytical Observation
Constitution of Pakistan (Art. 14(1))	"The dignity of man and, subject to law, the privacy of home shall be inviolable."	The conditional clause "subject to law" allows legislative limitation.	Partial recognises privacy but subordinates it to legislative authority.	Provides a normative basis but lacks an enforcement mechanism; open to restrictive interpretation.
PECA 2016	Sections 29, 32 on data retention and disclosure.	Broad executive powers to monitor and collect digital data.	Low proportionality safeguards or judicial oversight.	Expands state surveillance through discretionary language.
PTA 1996	No explicit privacy clause.	Allows interception "in the interest of national security or public order."	Low prioritises state security over individual rights.	Establishes surveillance infrastructure under a regulatory guise.
IFTA 2013	Surveillance permitted upon judicial warrant.	Secret applications by intelligence agencies; limited transparency.	Moderate provides procedural oversight but limited due process.	Judicial authorisation is procedural, not substantive.

Linguistic Constructions and the Legal Justification of Surveillance

When constitutional, statutory and all policy texts were observed through a critical discourse lens, it showed how language was used as a legitimising mechanism. In these texts, recurring



terms such as "public order," "national security," and "integrity of Pakistan" functioned as linguistic keys that unlocked unrestricted power. These terms seemed to have neutral value; however, they have ideological exposition that constructs the concept of surveillance as necessary and benevolent. The Constitution's phrase "subject to law," PECA's invocation of "public order," and IFTA's references to "lawful interception" form a discursive connection that naturalises invasion. Moreover, the expansion of such discursive construction through policy documents, including the National Cybersecurity Policy (2021) and the Digital Pakistan Vision, highlighted the concept of surveillance as an instrument of modernisation. Similarly, terms like "digital hygiene," "data sovereignty," and "cyber resilience" are used to depict surveillance as a protective and developmental necessity, and by using this type of language, privacy was redefined as a community good rather than an individual right. This displayed a crucial aspect in terms of moving the moral governance centre from liberty to control. Moreover, the citizens were reformed linguistically as right holders with the only responsibility of helping in monitoring themselves.

In addition to this, judicial discourse also played a very vital role in normalising this language, as in telephone interception cases, the courts have described surveillance as a "reasonable restriction" when national security is at stake. The phrase "reasonable restriction," in constitutional vocabulary, played the role of a legitimising device that transformed exception into an accepted norm. Moreover, this linguistic pattern was also observed in legislative drafting as PECA's use of expressions such as "whoever intentionally or unintentionally" and "may be prescribed" introduced vagueness that broadened the interpretive space for enforcement agencies. The same linguistic technique was evident in IFTA's provision, which seemed to allow interception when "necessary in the interest of national integrity." The elasticity of "necessary" ensures that almost any act of surveillance can be justified post hoc. Through this, the language became the main instrument of legal rationalisation, which, at other times, may be an unconstitutional intrusion into the acts of administrative legality.

Table 2: Discursive Construction of Privacy and Surveillance

Text Type	Dominant Phrases	Terms / Discursive Function	Ideological Effect
Constitutional Text	"Subject to law", "dignity of man", "privacy of home"	Frames privacy as conditional and domestic.	Limits privacy to physical space; legitimises legal intrusion.
Legislative Texts (PECA, IFTA, PTA)	"National security", "public order", "lawful interception"	Justifies surveillance as legal and patriotic.	Normalises surveillance through securitised vocabulary.
Judicial Discourse	"Reasonable restriction", "public interest", "integrity of Pakistan"	Balances privacy against state necessity.	Converts exceptions into norms through judicial reasoning.
Policy Documents	"Digital hygiene", "data sovereignty", "cyber resilience"	Presents surveillance as modernisation.	Rebrands surveillance as progress, erasing its coercive nature.



Discussion

Alignment Between Pakistani Legal Frameworks and Constitutional Guarantees of Privacy

The results indicate the existence of a structural imbalance between the constitutional guarantee of privacy in Pakistan and the surveillance ability instilled in the legislative provisions. While Article 14(1) of the Constitution declares that "the dignity of man and the privacy of home shall be inviolable," this protection is qualified by the phrase "subject to law," which, as (Humble, 2021; Kamenskii, 2024) observe, introduces a broad opening for state interference. This qualification has made privacy cease to be an inviolable right and a bargainable interest in the constitutional order of Pakistan. Theoretically, one of the foundations of autonomy and dignity is privacy (Newell, 1995; Schoeman, 1984), but in reality, the statutory regulation, including the Prevention of Electronic Crimes Act 2016 (PECA) and the Investigation for Fair Trial Act 2013 (IFTA), undermines the former by justifying the wide surveillance powers. The legislative phrasing of PECA 2016, especially in Sections 29 and 32, permits the retention and sharing of user data "for any period as may be prescribed," providing investigative agencies with nearly unrestricted power. As S. Khan et al. (2019) argue, these clauses condone the practices of over-surveillance and eventual suppression of civil rights in the name of national security.

The trend aligns with the international interests of unwarranted and excessive surveillance. Researchers, including (Rønn & Lippert-Rasmussen, 2020) maintain that the legitimacy of surveillance should be able to meet three criteria, i.e., legality, necessity, and proportionality. But in Pakistan, the surveillance laws only meet the former of these, which is the legality, and not the latter two. The proliferation of digital monitoring has grown exponentially, according to (Nandy, 2023; Verhelst et al., 2020) Much faster than the legal protections that are intended to make it accountable and avert the loss of the protective content of constitutional guarantees. Moreover, it is also steered towards this difference by the judicial interpretation of privacy. In *Benazir Bhutto v. Federation of Pakistan* (PLD 1988 SC 416), the Supreme Court elevated privacy as part of the "dignity of man," affirming that personal autonomy is central to democracy. This supplication of constitutional values demonstrated the state-centric proportionality doctrine, where the court evaluates the rights against security with an inclination towards executive interests. (Kamenskii, 2024).

However, in some scenarios privacy was acknowledged as "intrinsic to dignity," but did not encompass the protection against digital surveillance and data monitoring. This judicial hesitation showed that legal institutions often internalise surveillance narratives by perceiving monitoring as a protective necessity instead of a constitutional concern. (Büchi et al., 2022). Furthermore, there are no laws to protect the data, which are holistic and therefore increase the insecurity regarding privacy safeguards in Pakistan. (Sabri & Sabiri, 2023) Emphasised that Pakistan lacks a fully-fledged, ultra-modern data protection law that could be capable of addressing contemporary digital threats. This gap allowed the administrative authorities to make a general interpretation of surveillance requirements, which created an imbalance between privacy and security. (Nabeel & Iqbal, 2025). In addition to this, the constitutional language was aimed to protect the dignity, but instead it has been currently being utilised to promote invasion. The legislative and judicial discourse has also transformed this constitutional limitation into a legal justification for persistent surveillance. This dynamic highlighted the influence of digital colonialism, where domestic law replicated the external surveillance paradigm while neglecting the protection of individual rights. (Qamar, 2019).



Linguistic and Discursive Constructions Shaping Legal Justification

The linguistic analysis of the Constitution of Pakistan and statutory texts revealed that legitimization of surveillance is not solely a matter of legal design, but language also has a vital role in it. (N. L. Fairclough, 1985; Mullet, 2018) explained that law functioned as discourse as it was a structured system of meaning that reflected and reproduced power relations. In the Pakistani context, words such as "public order," "integrity of Pakistan," and "national security" served as discursive anchors that naturalised intrusion and made surveillance linguistically and morally acceptable. (Barnard-Wills, 2013) observed that linguistic framing allows states to construct surveillance as a "necessary and benevolent" act, an observation borne out by Pakistan's legislative lexicon. For instance, in the Pakistan Telecommunication (Re-organisation) Act 1996, interception is authorised "in the interest of national security or public order." There exists an ideological connotation of such seemingly neutral words, allowing discrete interpretation by authorities at their own will. The state thus presented surveillance as a measure of protection rather than intrusion, a strategy that aligned with (McDonald & Forte, 2021) concept of "utilitarian subordination," where privacy is reframed as a lesser social value in the pursuit of collective security. Moreover, this discursiveness is supported with the help of judicial language, as in *S. M. Zafar v. State*, the Court characterised interception as a "reasonable restriction," borrowing directly from constitutional terminology. The term "reasonable" functioned rhetorically to transform coercive practices into lawful governance. As (Riner, 2018) argued, such "semantic ambivalence" in legal language allowed states to move back and forth between rights-based rhetoric and security-oriented justification while maintaining legitimacy.

In addition to this, the policy discourse also promoted this normalization through technical vocabulary as the National Cybersecurity Policy (2021) used terms like "cyber hygiene," "resilience," and "data sovereignty." Moreover, (Selvam & González Vallejo, 2025) also highlighted that such language creates the illusion of responsible governance while the particular aim of it is to increase the authority of surveillance. The citizens were not considered right bearing but their role was only to cooperate in maintaining digital order. The discourse of "responsible digital citizenship" very delicately transferred the burden of compliance towards the individual and also made surveillance a shared civic duty. Furthermore, Critical Discourse Analysis (CDA) also helped to uncover power asymmetries produced through linguistic strategies. (Fairclough, 1985) three-dimensional model revealed that the repeated use of security-oriented language across legal and policy documents played a very significant role in making surveillance a part of social structure. The textual level represented vague statutory expression, and the discursive level highlighted the way surveillance was portrayed as protection. Moreover, the social level demonstrated the way citizens internalised this discourse as literal common sense.

This linguistic trend highlighted the global patterns observed in the literature as (Rønn & Lippert-Rasmussen, 2020) Cautioned that phrases like "protection of public order" often operated as euphemisms for expansive state power by creating ambiguity around proportionality. Such ambiguity in the interpretation of the law in Pakistan justified ex post surveillance as opposed to ex ante and further weakened the constitutional protections. Furthermore, these ideologically evident linguistic constructions made surveillance natural and ethical and made it a moral duty. In this regard, the discourse resulted in the establishment of the same social reality equating the authority of the state with its obligation to protect.



Similarly, this kind of interaction is highly evident in the explanation of digital governance in Pakistan, which associates surveillance with contemporary modernisation and accountability. The rhetoric of "digital security" and "cyber resilience" found in government communications positioned surveillance as an emblem of progress. (Barnard-Wills, 2013; Selvam & González Vallejo, 2025) Observed that such rhetoric reframes the expansion of control as a caring practice. Moreover, the findings also observed that legal and policy discourse in Pakistan was linguistically framed as an ideological tool for normalisation, as (McDonald & Forte, 2021) concluded that the language of security transforms coercion into consensus by allowing citizens to accept surveillance as a natural condition of civic life.

Summary of Findings

The analysis of constitutional texts, statutes, judicial interpretations, and policy discourse led to the following findings:

1. The constitution recognised privacy, but this was also undermined by its own conditional phrasing. The words “subject to law” permitted legislative intrusion and created a threat to privacy on governmental discretion.
2. Statutory instruments such as PECA 2016, PTA 1996, and IFTA 2013 implemented this choice by giving powers of interception and data collection without strict judicial supervision.
3. Judicial reasoning on one hand promoted privacy as intrinsic to dignity, yet also upheld surveillance practices under the justification of “reasonable restriction” and “public order”.
4. The linguistic framework of all these policy documents collectively constructs an ideology in which surveillance was considered a moral and administrative necessity.

Conclusion

The study highlighted a significant contradiction within the constitutional and legal landscape of Pakistan, as the constitution recognised privacy as a fundamental component of human dignity, but the legal and policy structures of the state consistently undermined it. Moreover, the linguistic structures of the constitution and legal documents transformed this protection into a conditional right that allowed the state to justify surveillance under the pretext of legality. Moreover, the study observed that there was use of vague terminologies to enable administrative discretion, which ultimately, instead of restraining the state authority, institutionalised it by converting security into a permanent justification for surveillance. In addition to this, the study also observed that the courts have acknowledged privacy as an integral part of dignity, but simultaneously deferred to executive powers in the name of national security in cases concerning telephone tapping and digital monitoring, where the understanding of privacy from the perspective of the judiciary remained cautious and fragmented. Furthermore, the study also concluded that there is a dire need for the establishment of coherence between constitutional principles and legal practice that can reform the statutory framework of the country and its discursive orientation. This can be done only through structural and linguistic transformation that can align the constitutional promise of dignity with the realities of digital governance and safeguard privacy in the age of pervasive surveillance.

References

Abbas, Z., Khan, R., Khan, M. Z., & Imran, M. (2023). *Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression*



- and Right to Privacy. *Journal of Creative Communications*.
<https://doi.org/10.1177/09732586231206913>
- Ali, M. I. (2025). From Sovereignty to Surveillance: The Legal Landscape of “Digital Colonialism” in India and Pakistan. *Vietnamese Journal of Legal Sciences*, 13(1), 67–81.
<https://doi.org/10.2478/vjls-2025-0005>
- Barnard-Wills, D. (2013). Security, privacy and surveillance in European policy documents. *International Data Privacy Law*, 3(3), 170–180. <https://doi.org/10.1093/idpl/ipt014>
- Bhat, P. I. (2020). Doctrinal Legal Research as a Means of Synthesizing Facts, Thoughts, and Legal Principles. In *Idea and Methods of Legal Research* (pp. 143–168). Oxford University Press Delhi. <https://doi.org/10.1093/oso/9780199493098.003.0005>
- Büchi, M., Festic, N., & Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society*, 9(1).
<https://doi.org/10.1177/205395172111065368>
- Chaara, I., Falisse, J.-B., & Moriceau, J. (2022). Does legal aid improve access to justice in ‘fragile’ settings? Evidence from Burundi. *Journal of Peace Research*, 59(6), 810–827.
<https://doi.org/10.1177/00223433211055633>
- Daudpota, F. (2016). Fundamental Scope of the Right to Privacy in Pakistan Need for a New Data Protection Law. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2866416>
- Eppley, K. (2019). Close reading: What is reading for? *Curriculum Inquiry*, 49(3).
<https://doi.org/10.1080/03626784.2019.1631701>
- Fairclough, N. (2013). Critical discourse analysis and critical policy studies. *Critical Policy Studies*, 7(2). <https://doi.org/10.1080/19460171.2013.798239>
- Fairclough, N. L. (1985). Critical and descriptive goals in discourse analysis. *Journal of Pragmatics*, 9(6), 739–763. [https://doi.org/10.1016/0378-2166\(85\)90002-5](https://doi.org/10.1016/0378-2166(85)90002-5)
- Gay, L. R., Mills, G. E., & Airasian, P. W. (2008). *Educational Research: Competencies for Analysis and Applications* (10th ed.). Pearson.
- Golafshani, N. (2015). Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*. <https://doi.org/10.46743/2160-3715/2003.1870>
- Hayat, M. A. (2007). Privacy and Islam: From the Quran to data protection in Pakistan. *Information & Communications Technology Law*, 16(2), 137–148.
<https://doi.org/10.1080/13600830701532043>
- Humble, K. P. (2021). International law, surveillance and the protection of privacy. *The International Journal of Human Rights*, 25(1), 1–25.
<https://doi.org/10.1080/13642987.2020.1763315>
- Hunter, L. (2016). Making time and space: The impact of mindfulness training on nursing and midwifery practice. A critical interpretative synthesis. In *Journal of Clinical Nursing* (Vol. 25, Issues 7–8). <https://doi.org/10.1111/jocn.13164>
- Jabeen, T. (2021). Right of Privacy: The Lacuna in Pakistan and Indian legal Framework. *Pakistan Languages and Humanities Review*, 5(II), 460–471.
[https://doi.org/10.47205/plhr.2021\(5-II\)2.35](https://doi.org/10.47205/plhr.2021(5-II)2.35)
- Kamenskii, M. A. (2024). Constitutional legal limits to privacy protection. *Proceedings of Southwest State University. Series: History and Law*, 14(3), 48–60.
<https://doi.org/10.21869/2223-1501-2024-14-3-48-60>
- Khan, A. J., Mushtaq, S. A., Siddique, M. A., & Wadood, M. A. (2025). The Right to be forgotten in the Digital Age: A Pakistani Perspective on Balancing Data Protection



- & Privacy, Freedom of Expression, and Cyber Security. *Journal for Social Science Archives*, 3(1), 387–403. <https://doi.org/10.59075/jssa.v3i1.126>
- Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 Provisions on Freedom of Speech: A Case of Pakistan. *Journal of Management Info*, 6(2), 7–11. <https://doi.org/10.31580/jmi.v6i2.566>
- Lever, A. (2006). Privacy Rights and Democracy: A Contradiction in Terms? *Contemporary Political Theory*, 5(2), 142–162. <https://doi.org/10.1057/palgrave.cpt.9300187>
- Ludovico, A. B., Banfi, F., Losa, S., Petralia, F., Speroni, E. F., Ghisi, A., & Mariani, S. (2022). Reliability. In *Silicon Sensors and Actuators: The Feynman Roadmap*. https://doi.org/10.1007/978-3-030-80135-9_26
- McDonald, N., & Forte, A. (2021). Powerful Privacy Norms in Social Network Discourse. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–27. <https://doi.org/10.1145/3479565>
- Mullet, D. R. (2018). A General Critical Discourse Analysis Framework for Educational Research. *Journal of Advanced Academics*, 29(2), 116–142. <https://doi.org/10.1177/1932202X18758260>
- Nabeel, F., & Iqbal, K. (2025). Privacy, Data Protection and Cyber Crimes: Mapping Perceptions of Pakistani Users. *Journal of Applied Security Research*, 20(2), 293–319. <https://doi.org/10.1080/19361610.2024.2372989>
- Nandy, D. (2023). Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns. *Journal of Current Social and Political Issues*, 1(1), 13–17. <https://doi.org/10.15575/jcspi.v1i1.442>
- Newell, P. B. (1995). Perspectives on privacy. *Journal of Environmental Psychology*, 15(2), 87–104. [https://doi.org/10.1016/0272-4944\(95\)90018-7](https://doi.org/10.1016/0272-4944(95)90018-7)
- Nisar, M. A., & Asghar, M. S. (2025). Privacy as a Legal Right: A Comparative Study Between Pakistan and Malaysia. *Journal of Arts and Linguistics Studies*, 3(1), 839–858. <https://doi.org/10.71281/jals.v3i1.254>
- Praditama, I. B. M., & Ranawijaya, I. B. E. (2023). The role of international law in preventing and addressing human trafficking from the perspective of the right to privacy under ICCPR. *POLICY, LAW, NOTARY AND REGULATORY ISSUES (POLRI)*, 2(3), 198–207. <https://doi.org/10.55047/polri.v2i3.620>
- Qamar, A. U. H. (2019). Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan. *International Journal of Computer Network and Information Security*, 11(1), 62–69. <https://doi.org/10.5815/ijcnis.2019.01.06>
- Riner, R. C. (2018). Legal Language. In *The International Encyclopedia of Anthropology* (pp. 1–2). Wiley. <https://doi.org/10.1002/9781118924396.wbiea1400>
- Rønn, K. V., & Lippert-Rasmussen, K. (2020). Out of Proportion? On Surveillance and the Proportionality Requirement. *Ethical Theory and Moral Practice*, 23(1), 181–199. <https://doi.org/10.1007/s10677-019-10057-z>
- Sabri, M. N., & Sabiri, M. S. (2023). Cyber Security in Current Era in Pakistan: An Analysis of Cyber-Crimes and Cyber-Laws of Pakistan. *Pakistan's Multidisciplinary Journal for Arts & Science*, 4(2), 64–79. <https://doi.org/https://doi.org/10.5281/zenodo.8105463>
- Schoeman, F. (1984). Privacy: philosophical dimensions of the literature. In *Philosophical Dimensions of Privacy* (pp. 1–33). Cambridge University Press. <https://doi.org/10.1017/CBO9780511625138.002>



- Selvam, M., & González Vallejo, R. (2025). Ethical and Privacy Considerations in AI-Driven Language Learning. *LatIA*, 3, 328. <https://doi.org/10.62486/latia2025328>
- Shah, S. A. A., & Butt, M. N. (2025). Pakistan's PECA 2025 and Global Digital Regulations: Balancing Security and Freedom. *Social Prism*, 2(01), 64–91. <https://doi.org/10.69671/socialprism.2.1.2025.28>
- Van Dijk, T. A. (1993). Principles of critical discourse analysis. *Discourse & Society*, 4(2). <https://doi.org/10.1177/0957926593004002006>
- Verhelst, H. M., Stannat, A. W., & Mecacci, G. (2020). Machine Learning Against Terrorism: How Big Data Collection and Analysis Influences the Privacy-Security Dilemma. *Science and Engineering Ethics*, 26(6), 2975–2984. <https://doi.org/10.1007/s11948-020-00254-w>
- Yongmei, C., & Afzal, J. (2023). Impact of Enactment of 'The Prevention of Electronic Crimes Act, 2016' as Legal Support in Pakistan. *Academy of Education and Social Sciences Review*, 3(2). <https://doi.org/10.48112/aessr.v3i2.500>