INTERNATIONAL JOURNAL OF SOCIAL SCIENCES BULLETIN
ISSN: (E) 3007-1917 (P) 3007-1909
Volume 4, Issue 2, 2026

DATA PRIVACY IN PAKISTAN: A COMPARISON OF LEGAL LANDSCAPE WITH THE EUROPEAN UNION

Hafiz Abdul Razzaq[1], M. Abu Bakar Chandia[*2]

[1]*Advocate High Court, LL.M. (Constitutional Law), University of the Punjab*
[*2]*Final Year Law Student, University Law College, PU*

[1]abdulrazzaqpulclhr43@gmail.com ,[*2]abubakarchandia123@gmail.com

Corresponding Author: *
M. Abu Bakar Chandia
DOI: https://doi.org/10.5281/zenodo.18617039

Received	Accepted	Published
12 December 2025	27 January 2026	12 February 2026

ABSTRACT

Personal data is now highly in demand with the introduction of digital technology and that is why there is need of data privacy. The sudden rise of digital systems in Pakistan, both in the public sector and in the business has not been coupled with tough data protection legislations. Due to this there are gigantic breaches in processing of personal data and this is what leaves citizens vulnerable to abuse of data and governmental surveillance. The paper will compare the current legislations and the proposed legislations protecting data in Pakistan. It takes into consideration the Prevention of Electronic Crimes Act (PECA) 2016 and the Personal Data Protection Bill (PDPB) 2023. These legislations are compared to European Union (EU) legislations and specifically, the General Data Protection Regulation (GDPR), Digital Markets Act (DMA), Artificial Intelligence Act (AI Act) and European Convention on Human Rights (ECHR). The research shows that the legislation in Pakistan in terms of data protection is flawed. Instead of focusing on the protection of the rights of people, it is centred more on the interests of the state. Enforcement is loosely controlled, there is too much centralization of the power within the state and unclear laws on the consent of people being acquired. In turn, the legal system does not comply with the international standards. The paper argues that the data legislations in Pakistan steal the vocabulary of the global laws, but lack in their content and values.

Keywords: *Data Privacy, Data Protection Laws, Digital Constitutionalism, GDPR, State Surveillance*

Introduction

The twenty-first century is defined by the proliferation of information and communication technologies (ICT), which has elevated personal data into the most valuable resource of the digital economy, simultaneously making it the prime target of surveillance and exploitation. This reality has necessitated a fundamental reassessment of the human right to privacy—a right first conceived in terms of physical space but now overwhelmingly defined by the control an individual hold over their digital footprint in an era described as 'surveillance capitalism'. Jurisdictions globally have struggled to regulate this environment, but the European Union (EU), through its robust legal architecture, has established itself as the preeminent global standard for data protection. Pakistan, mirroring global trends, is undergoing rapid digital transformation, driven by e-governance initiatives, widespread biometric registration, and a burgeoning digital economy. However, this progress has not been matched by a coherent legal framework. While the Constitution of the Islamic Republic of Pakistan, 1973, affirms the inviolability

of human dignity and privacy under Article 14, judicial efforts to apply this right to the digital sphere—notably in landmark cases such as Mohtarma Benazir Bhutto v President of Pakistan and Justice Qazi Faez Isa v President of Pakistan, have been consistently undercut by deficient legislative mechanisms. The primary governing statute, the Prevention of Electronic Crimes Act, 2016 (PECA), is structurally flawed, prioritizing state authority, facilitating mass data retention, and granting overly broad immunity to service providers. The introduction of the Personal Data Protection Bill (PDPB), 2023 represents an attempt to align Pakistan with international norms, yet critical analysis reveals significant structural weaknesses, including sweeping national security exemptions and a regulator structurally dependent on the executive. These domestic limitations necessitate a rigorous legal comparison. This study's central objective is to provide a systematic comparative analysis of the data protection legal landscapes in Pakistan and the European Union, demonstrating how the latter's rights-based approach exposes the fundamental gaps in the former. The European Union's legislative and judicial approach to data privacy is characterized by its proactive, rights-based positioning of personal data protection as a fundamental human right. This framework, rooted in the European Convention on Human Rights (ECHR), is operationally defined by the General Data Protection Regulation (GDPR) and continually refined through the stringent oversight of the Court of Justice of the European Union (CJEU). The EU has recently expanded its regulatory scope through the adoption of the Digital Markets Act (DMA) and the Artificial Intelligence Act (AI Act), forming a comprehensive "Digital Rulebook" designed to govern the entire digital environment, from market structure to algorithmic decision-making.

Key analyses demonstrate that the framework enforces a strict necessity and proportionality test for state surveillance activities, demanding independent judicial review before access to citizens' communications data. Furthermore, the extraterritorial effect of the GDPR, particularly through its requirements for international data transfers, continues to export EU standards globally, exemplified by the stringent enforcement actions following the *Schrems II* judgment and the continuous legal instability surrounding the EU-US Data Privacy Framework (DPF). The synthesis of these legislative mandates, judicial restraints, and technologically responsive regulations confirms the EU's proactive strategy to govern the digital domain, balancing state security needs with individual autonomy and corporate power.

By identifying the critical legal and institutional deficiencies in Pakistan relative to these EU standards, this paper argues that the Pakistani framework is inadequate for the modern digital age. The ultimate goal of this research is to leverage this comparative analysis to formulate a sophisticated blueprint for policy reform in Pakistan. This blueprint proposes a robust, rights-based system of data protection that is internationally viable, capable of meeting the stringent requirements for EU adequacy for cross-border data transfers, and is structurally designed to protect citizens' fundamental rights.

Literature Review

Essentially, new forms of economic activity that are characterized by Surveillance capitalism as outlined by Shoshana Zuboff (2019) may be characterized by the fact that personal data is mined and gathered and can be utilized to make assumptions and control people, which is dangerous to even the existence of privacy. It is a global phenomenon due to which the protection of the data now becomes not only a technical problem, but also a pressing human rights problem. The norm of the right to privacy is stated in the article 14 (1) of the Constitution, and the courts in Pakistan broadly interpreted the provision. The Supreme court judgments in Benazir Bhutto case and in Justice Qazi Faiz Isa case, the court have diligently expanded this right from the physical space, to the technological and cyber space and in the latter case the court in its categorically stated that data at the cyber space is sacrosanct against unwarranted invasion.

However, despite the giant constitution and judicial framework, scholars perceive that the law-making system in Pakistan is an errant under-

achiever in as much as the demands are concerned. Muhammad Hammad Amin and Maira Hassan (2021) in their article in LUMS Law Journal propose the assumption that the currently existing law proves inadequate in ensuring the safety of the data of citizens. PECA 2016 has been largely criticized as a law that motivates the state to spy on the privacy of the individual in a bid to counter the cybercrimes. Equally, the PDPB, though on the right track, was proposed at the time that has failed to escape criticism due to its sweeping exemption of the government agencies and the unavailability of good execution, the characteristics of the best practices of the world. The other point made by Aly Hassam Ul Haq is that the huge exemptions made out in the bill such as the one made by section 24 of the bill was more about state power than the protection of the people. Scholars also argues that Pakistan's legal landscape is insufficient for the Artificial Intelligence(AI) era. Areeba Iqbal Qureshi (2023) notes that although the draft National AI Policy includes an 'AI Regulatory Directorate' under the future National Commission for Personal Data Protection (NCPDP), the Commission has not been established yet and all this protection is therefore purely theoretical. She cautions that without an effective governance structure, the digital space in Pakistan is prone to the unchecked nudging and consent fatigue where the user is engineered into the state of forfeiting their privacy devoid of meaningful agency.

The most vital point of reference of such standards across the borders would be the GDPR of EU. The GDPR also presented a number of generalized ideas such as data minimization and consent of users, considering it to be the best in the global system (based on the model of human rights, built on the principles of Article 8 of ECHR). It is both a legislative and technical norm against which the amount of legislative work of state as Pakistan can be judged.

Based on the premises of GDPR, and with the primary aim of taking additional control over the information habits of digital platform commonly referred to as gatekeepers, EU also come up with Digital Markets Act (DMA). It is first of all, a competition tool, but it has a few provisions concerning data privacy. An example is the article 5(2) which barricades the retrieval of data on other platforms by the gatekeepers without the knowledge and consent of the user. The EU has also enacted the AI Act, which has been the first ever legislation to be targeted at resolving the problems posed by artificial intelligence. This once again makes the EU the driving force, and the world must assume the lead.

Therefore, the current literature on the issue remains scant, despite several reports pointing to the difference existing between the developing laws on data protection in Pakistan and the GDPR in the EU. A significant body of literature considers data protection as a discrete compliance activity without connecting it to the larger problems of tech company market power, and new technologies and their threats. It is evident that there is no extensive literature of juxtaposing the legal landscape of Pakistan with what can be referred to as the evolving European trilogy of laws in the form of the GDPR rings of rights-based protections, the Digital Markets Act (DMA) of the EU in checking market hegemony, and the risk-driven provisions of the AI Act.

This research paper will fill that gap. In asking the question of how these combined international standards relate to the legal provisions of Pakistan on this question, the paper transcends the yes or no analysis. Rather, it provides an extensive criticism of the failure of the current strategy being pursued by Pakistan, where much of the effort is put into self-regulation by the industry and policies led by the government, to respond to the realities of the market today, which is highly based on surveillance.

Section 1: The Foundational Bipolarity of European Data Law

The architecture of European data protection law rests on two interdependent pillars: the constitutional grounding in human rights law and the practical implementation through comprehensive regulatory statutes. This duality ensures that data protection remains a principled defense of human dignity rather than merely a technical compliance exercise.

1.1 The Constitutional Bedrock: Article 8 of the ECHR and the Charter of Fundamental Rights

The foundational premise for privacy protection in Europe is enshrined in Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for an individual's "private and family life, home and correspondence". This constitutional provision is critical because it ensures that any intrusion upon private life by public authorities must satisfy three demanding, cumulative criteria: the interference must be provided "in accordance with the law," must pursue a legitimate goal (such as national security or public order), and, most significantly, must be "necessary in a democratic society" (the principle of proportionality).

The interpretation of this provision by the European Court of Human Rights (ECtHR) has historically been expansive. For instance, the ruling in *Malone v. The United Kingdom* (1984) established that even when a surveillance regime is based on domestic law, the law itself must meet specific qualitative standards of clarity and foreseeability. This qualitative requirement prevents states from relying on vague administrative discretion. Consequently, the European system treats privacy as a fundamental boundary against the state, forcing governments to stringently justify all surveillance and data collection activities against the backdrop of fundamental rights.

1.2 The Legislative Architecture: GDPR as the Gold Standard for Informational Privacy

The General Data Protection Regulation (GDPR) operationalizes the constitutional right to privacy within the modern digital economy. It defines personal data broadly as "any information relating to an identified or identifiable natural person," encompassing online identifiers and location data. The GDPR establishes a set of strict processing principles in Article 5 that serve as the ethical and legal mandate for all data controllers.

These principles mandate that data processing must adhere to Lawfulness, Fairness, and Transparency; it must be subject to Purpose Limitation (processed only for explicitly specified goals); and it must adhere to Data Minimization (collecting only the data absolutely necessary). Furthermore, the principle of accountability is foundational, requiring controllers not just to comply with the rules but to demonstrably prove that compliance, typically through documentation and the mandatory implementation of Data Protection by Design and by Default. This structure forces organizations to integrate privacy safeguards into the technological architecture of their systems from the outset.

The GDPR shifts the paradigm of data governance by providing individuals, termed 'data subjects,' with a strong catalog of enforceable rights, thereby transferring control over digital identities back to the person. These rights, outlined in Chapter 3 of the Regulation, include the Right of Access (Subject Access Request), the Right to Rectification, the Right to limit Processing, and the Right to Data Portability.

Perhaps the most recognized is the Right to Erasure, or the Right to be Forgotten, a concept cemented by the CJEU's 2014 ruling in *Google Spain SL v AEPD and Mario Costeja González*. This right allows individuals to demand the deletion of personal data when it is no longer necessary for the original purposes or when consent is withdrawn. The inclusion of the Right to Data Portability, which enables users to obtain their data in a structured, machine-readable format and transfer it to another service provider without hindrance, signifies a fundamental conceptual shift. Pre-GDPR frameworks predominantly focused on preventing data misuse; however, the comprehensive rights under the GDPR, particularly portability and objection, emphasize individual empowerment. This capability allows users to challenge corporate data lock-in and encourages market competition based on compliance, an operational objective that directly supports the goals later formalized in the Digital Markets Act (DMA). The legal instrument is thus designed to be a potent tool for individual autonomy in the digital age.

Section 2: Judicial Dialectics: Limiting State Power and Mass Surveillance

The European courts, particularly the CJEU and the ECtHR, play an essential role in defining the boundary between legitimate state security measures and the fundamental rights of privacy and data protection. This role is most evident in the

jurisprudence concerning governmental access to electronic communications data, often claimed under the broad rubric of national security.

2.1 The CJEU's Red Lines: The Invalidation of General and Indiscriminate Data Retention

A core feature of the European framework is the judicial rejection of mass surveillance measures. The CJEU established a clear red line in its landmark rulings, beginning with *Digital Rights Ireland* (2014), where it invalidated the EU Data Retention Directive. This jurisprudence was solidified in *Tele2 Sverige* and *Watson* (2016), where the Court unequivocally declared that the general and indiscriminate retention of traffic and location data is unlawful.

The Court classified such blanket data harvesting as a "particularly serious interference" with fundamental rights because the metadata—which includes communication times, location, and recipients—allows for "very precise conclusions to be drawn concerning the private lives" of the individuals concerned. The retention was deemed disproportionate as it encompassed all citizens, irrespective of any suspicion of serious criminal activity. The ruling demanded that any data retention measure, even for the purposes of fighting serious crime, must be strictly *targeted* by subject, time, means, and geographical area, and must be proportionate to the objective pursued. This effectively dismantled previous efforts by Member States to utilize mass data retention as a generalized tool for law enforcement.

The CJEU continued this judicial dialogue in the *La Quadrature du Net II*-Judgment, issued in 2024. This ruling addressed the nuanced legal status of different categories of retained data, particularly Internet Protocol (IP) addresses, which are considered less intrusive than location or traffic data. The Court demonstrated a degree of judicial pragmatism by confirming that national security could justify the preventive retention of data of *all* users if limited to a foreseeable period.

Crucially, the Court determined that the general and indiscriminate retention of IP addresses was permissible and did not necessarily constitute a "serious interference" with fundamental rights, even extending this possibility to cases involving "lesser crimes," such as infringements of intellectual property rights committed exclusively online. This decision represents a nuanced application of the proportionality test, distinguishing between data that reveals deep insights into private life (location/traffic data) and data that might be less sensitive (IP addresses). However, this allowance is carefully conditional: the retention must be limited to circumstances where the possibility of serious interference in the private life of the person concerned can be "genuinely ruled out," and it is subject to the specific provisions and safeguards enshrined in the respective national law. This move has been interpreted by some legal scholars as a tactical concession aimed at harmonizing the CJEU's position with certain national constitutional court perspectives, thereby navigating the delicate constitutional dialogue on state security powers. On the other hand, some argue that this decision fails to explain in sufficient depth the relationship between the collection and processing of low-sensitivity data and their subsequent use by state authorities.

2.2 Safeguards and Accountability: The Necessity of Independent Review

Despite the occasional allowances for necessary, targeted data retention, the judiciary consistently emphasizes that strong procedural safeguards are the core requirement for legitimacy. The ECtHR's *Zakharov* criteria established minimum legal requirements for surveillance regimes, including precise guidance on the types of offenses and subjects, restrictions on the time limit of interception, and adequate procedures for data disposal.

The CJEU further affirmed that access to any retained data—whether traffic data or IP addresses—must be strictly restricted to fighting serious crime and must be subjected to *prior review* by an independent administrative authority or a court, whose ruling is binding. This procedural requirement ensures that state access to private data is not arbitrary but must pass a rigorous necessity and proportionality test sanctioned by an impartial body. This institutional mechanism is the primary defense against state overreach, making the *process* of surveillance authorization as critical as the legal

basis for the measure itself. The tension between national security policy, such as the UK's Investigatory Powers Act (IPA) 2016, and the supremacy of EU privacy law, demonstrated by the IPA's incompatibility with EU standards post-*Watson*, continues to underscore the judiciary's restrictive posture toward mass surveillance.

Section 3: The New Digital Rulebook: Cohesion and Tension in Complementary Legislation

The European Union has moved beyond the GDPR to create a comprehensive "Digital Rulebook," addressing the structural power of large technology companies and the pervasive risks posed by artificial intelligence. This strategy involves the seamless integration of GDPR principles into the Digital Markets Act (DMA) and the Artificial Intelligence Act (AI Act).

3.1 GDPR and the Digital Markets Act (DMA)

The DMA, which targets major online platforms designated as "gatekeepers," complements the GDPR by addressing market contestability and fairness, two issues that fundamentally impact the free exercise of data rights. While the GDPR focuses on protecting individual rights (e.g., controlling consent), the DMA aims to prevent gatekeepers from abusing their dominant positions to enforce more stringent operational standards, particularly regarding transparency and user privacy.

The synergy between the two laws is substantial. The DMA requires gatekeepers to secure clear and informed consent, aligning precisely with GDPR principles, especially when combining or reusing data across different services they operate. The legislative strategy here is innovative. The GDPR primarily operates *ex-post*, penalizing companies after a breach or violation occurs through fines. The DMA, conversely, acts *ex-ante* by preemptively restructuring market conduct. It recognizes that in highly dominant digital environments, a user's "consent" often lacks the voluntariness necessary for it to be truly free and informed under the GDPR. By demanding structural changes like enhanced user control and stricter rules on data combination, the DMA creates a market-based defense of privacy, ensuring that compliance is built into the competitive structure of the market. The European Data Protection Board (EDPB) and the European Commission are actively developing joint guidelines to clarify these common touchpoints and ensure consistent application.

3.2 AI Act and GDPR

The AI Act establishes a horizontal framework governing the safety and fundamental rights implications of artificial intelligence systems, with specific attention given to high-risk systems (HRS). The AI Act is deeply integrated with the GDPR, often requiring the layering of new obligations onto existing data protection requirements.

One area of significant overlap is accountability and risk assessment. The GDPR already requires that certain high-risk processing operations undergo a Data Protection Impact Assessment (DPIA). The AI Act explicitly mandates that deployers of high-risk AI systems must use information gathered under Article 13 of the AI Act to comply with their pre-existing GDPR obligation to carry out a DPIA, as stipulated in Article 26(8) AI Act. Furthermore, the AI Act introduces a **Fundamental Rights Impact Assessment (FRIA)** for HRS listed in Annex III. The requirement for a dedicated FRIA signifies that the EU views the potential harms of advanced AI (such as systemic bias, discrimination, or threats to democratic freedoms) as extending beyond the scope of mere data privacy infringements addressed in a DPIA. This regulatory sophistication demands a holistic review of algorithmic governance against all fundamental rights, not just informational privacy.

3.3 Digital Services Act

The Digital Services Act (EU) 2022/2065 seeks to establish a safer internet environment and safeguard the fundamental rights of the users through the establishment of new transparency and accountability responsibilities of the online platforms functioning in the EU. The DSA also mandates that platforms disclose and describe advertisements, and that they cannot use sensitive personal information (like religion or sexual orientation) to target ads, which decreases invasive profiling and also requires systems to allow researchers and regulators to understand how the

algorithmic systems work and access some information about that work, meaning that personal data whose processing is subject to DSA requirements remains safeguarded by the EU privacy law.

These acts also address algorithmic autonomy. The GDPR provides individuals with the right not to be subject to a solely automated decision that produces significant legal or similarly significant effects on them, allowing them to request human intervention. The AI Act strengthens this through Article 14, which establishes a more robust regime requiring high-risk AI systems to be designed with effective human-machine interface tools that enable competent personnel to exercise meaningful oversight. This continuous regulatory evolution demonstrates a strategy to ensure that technological advancements are always subordinate to human rights and accountability principles.

Section 4: The Extraterritorial Imperative: Global Transfers and Sovereignty

The EU's assertion of its data protection standards extends globally through Chapter V of the GDPR, which governs international data transfers. This extraterritorial reach has created significant legal and geopolitical tension, particularly concerning the flow of data to the United States.

In a recent development, the European Commission announced on 15 January 2024 that it has concluded its review of 11 existing adequacy decisions, confirming that personal data transferred to jurisdictions like Canada, Israel, and Switzerland continues to benefit from adequate data protection safeguards, demonstrating the EU's continuous monitoring of global data protection standards.

The landscape of transatlantic data transfers has been fundamentally shaped by the series of judgments named after privacy activist Maximilian Schrems. The *Schrems II* decision (2020) by the CJEU invalidated the EU-US Privacy Shield, the second successive transfer mechanism to be overturned. The Court held that US surveillance law did not provide protections "essentially equivalent" to those afforded in the EU, nor did it ensure satisfactory legal redress for EU citizens against US intelligence agencies.

This ruling underscored a critical principle: national security exceptions cannot be used to justify unlimited access to personal data, and any transfer mechanism must respect the "essence" of the fundamental rights to privacy and data protection guaranteed under the EU Charter. The invalidation created immediate legal uncertainty for thousands of companies and necessitated a complete restructuring of data flows between the two economic blocs.

4.2 The EU-US Data Privacy Framework (DPF 2023)

In response to *Schrems II*, the current EU-US Data Privacy Framework (DPF) was formalized in 2023 through an adequacy decision by the European Commission. The DPF attempts to address the CJEU's concerns by institutionalizing stronger limitations on US intelligence access, restricting collection to what is "necessary and proportionate" for clearly defined national security purposes. Furthermore, the framework established new oversight mechanisms, including an independent Data Protection Review Court (DPRC), intended to provide improved procedures for EU individuals to seek redress for improper data handling.

Despite the formal adequacy decision, legal challenges to the DPF were anticipated and are ongoing, raising questions about its long-term stability. The DPF is widely viewed by some analysts as a "quick, contractual 'fix'" adopted to accommodate US commercial and intelligence priorities rather than a fundamental legislative change to US surveillance laws. This chronic instability arises because the US legal structure concerning national security and data access remains structurally divergent from EU constitutional values. The CJEU's historical willingness to prioritize fundamental rights over commercial convenience suggests that the "ghosts" of the *Schrems* decisions may continue to challenge the current framework, requiring companies to remain cautious and vigilant to ongoing changes.

4.3 The Necessity of Transfer Impact Assessments (TIAs)

Following the *Schrems II* decision, the European Data Protection Board (EDPB) issued guidance that immediately impacted other transfer mechanisms, including Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). The EDPB made clear that there was no grace period, and data exporters using these mechanisms must conduct a Transfer Impact Assessment (TIA) prior to transferring data to a non-EEA jurisdiction.

The TIA places a heavy technical and legal burden on the data exporter. The exporter must rigorously assess the third country's legislation, particularly governmental access laws, focusing on whether that access "is limited to what is necessary and proportionate in a democratic society" and whether data subjects are afforded effective redress. The assessment must not rely on "subjective factors" like the perceived low likelihood of governmental access. If the third country's laws fail to meet the standard of essential equivalence, the exporter is responsible for identifying and adopting supplementary technical or contractual measures. These measures might include strong encryption where the key remains solely with the EU exporter, or contractual clauses requiring the data importer to challenge the legality of any order to disclose the data. This process effectively forces compliance with EU fundamental rights standards globally, making data protection a critical element of international commerce and trade.

Section 5: Enforcement, Accountability, and Financial Deterrence

The operational success of the GDPR framework relies on strong, independent enforcement mechanisms backed by significant financial penalties. This section analyzes the role and challenges of the Supervisory Authorities (SAs) and the measurable impact of accountability provisions.

5.1 The Role and Independence of Supervisory Authorities (SAs)

The structural integrity of GDPR enforcement hinges on the Supervisory Authority (SA) mandated in every Member State, such as the Data Protection Commission (DPC) in Ireland. These SAs are the primary enforcers, possessing extensive investigatory, advisory, and corrective powers, including the authority to impose massive administrative fines. Article 52 of the GDPR explicitly demands that each SA must act with "complete independence" and be "free from external influence, whether direct or indirect," to ensure impartiality in their decisions, especially when investigating government bodies or powerful corporations.

However, the SAs face significant structural and operational challenges. Research indicates that inadequate resources risk undermining both the effectiveness of their mandates and their required independence. Furthermore, the sheer volume of complaints lodged by data subjects presents a major administrative challenge that must be addressed as a priority. This operational constraint highlights a paradox of enforcement: while the law establishes massive financial deterrents against high-profile violations by multinational corporations, the routine handling of large numbers of individual complaints and the consistent supervision of complex data processing operations can be strained by resource limitations.

5.2 Accountability in Action: Mandatory Notification and DPIA

The principle of accountability demands transparency concerning security failures. The GDPR establishes a strict, two-tiered mandatory notification regime for personal data breaches. First, the data controller must notify the relevant Supervisory Authority "without undue delay and, where feasible, within 72 hours of having become aware thereof". Second, if the breach is "likely to result in a high risk to the rights and freedoms of natural persons," the controller must also inform the affected data subjects directly without delay. This system ensures that organizations cannot conceal security failures and that individuals are informed rapidly enough to take mitigating action.

Accountability is also enforced proactively through Data Protection Impact Assessments (DPIAs), which are mandated for high-risk processing activities. As noted, this obligation is now augmented by the AI Act's Fundamental Rights Impact Assessment (FRIA), demonstrating a continuous deepening of the EU's commitment to

ex-ante risk management that must cover not just data integrity but also broader human rights implications.

5.3 Analysis of Landmark Penalties (2021-2024)

The threat of severe financial consequences is the primary mechanism for ensuring corporate compliance globally. The maximum penalty for violations of fundamental principles or data subjects' rights is up to €20 million or 4% of the organization's total worldwide annual turnover, whichever is higher. Recent enforcement actions confirm the rigorous application of these fines, demonstrating a clear willingness to impose financial deterrence on even the largest global technology companies.

The historic €1.2 billion fine against Meta Platforms Ireland in May 2023 for illegal data transfers to the United States serves as a powerful demonstration of the extraterritorial force of the GDPR, confirming that non-compliance with cross-border rules carries severe financial penalties. The penalty levied against Amazon for infringing consent rules related to advertising targeting further underscores that the EU prioritizes the foundational principles of transparency and informed consent, holding large platforms accountable for systemic failures. These actions ensure that the Regulation remains a global benchmark, forcing multinational firms to adhere to EU standards irrespective of where they are headquartered.

Sustaining Rights in the Face of Technological Velocity

The European legal framework for data privacy provides a comprehensive, multi-layered defense against both unchecked state surveillance and commercial exploitation of personal data. Its strength derives from the synergy between constitutional rights (ECHR), stringent legislation (GDPR, DMA, AI Act), and an activist judiciary (CJEU).

The analysis reveals that the core regulatory challenge remains managing the dynamic tension between national security imperatives and fundamental human rights. The CJEU has succeeded in placing clear, judicially enforceable limits on general and indiscriminate state data retention, thereby guaranteeing that surveillance remains the exception rather than the rule. Simultaneously, the recent legislative expansion into the Digital Rulebook, notably the DMA and the AI Act, represents a forward-looking strategy that integrates privacy protection into the structure of digital markets and algorithmic design, moving beyond mere data flow regulation to govern technological capabilities themselves.

However, the framework's most acute operational vulnerability lies in the stability of international data transfers. The cycle of temporary adequacy decisions, such as the DPF, reflects a chronic geopolitical misalignment that forces EU data exporters to perpetually manage legal risk through costly Transfer Impact Assessments. Internally, the effectiveness of the expanded Digital Rulebook depends critically on ensuring that Supervisory Authorities are adequately resourced and capable of coordinating complex, multi-sector enforcement actions against globally dominant entities. Ultimately, the sustainability of the EU model hinges on its capacity to combine the financial deterrent of large fines with the consistent, routine application of fundamental rights protections across all levels of the digital ecosystem.

Transposing the EU's Rights-Based Digital Model into Pakistan's Legal Reality

Although the European Union has been on the path toward creating a unified rights-based digital architecture with the GDPR and the AI Act, the legal process in Pakistan is a challenging endeavor of balancing a constitutional reverence towards human dignity with the national security imperatives. This moves to the ideas of the EU gold standard to the Pakistani terrain unveils a change in proactive, protective model, to a framework that leans towards the reactive interpretation of the law and a heavy dependence on subordinate legislation.

Section 6: Pakistan, The Constitutional Mirage: Art 14 and the "Subject to Law" Paradox

Privacy protection in Pakistan is anchored on ethical and constitutional principles that are well laid down in the supreme law. In the Constitution

of Islamic Republic of Pakistan 1973, article 14(1) provides that, "the dignity of man and, subject to law, the privacy of home, shall be inviolable". Privacy is known in this provision as an untenable part of human dignity. The effectiveness of this promise in the constitution is however very quickly undermined by the clause whereby it is subject to law and this gives a paradoxical effect with a core right coming to be subordinate to the quality of the legislations made by the parliament.

6.1 The Judicial Vanguard: Expanding the Privacy Frontier

The courts, through the Supreme Court of Pakistan have been instrumental in construing Article 14 on a figurative or spatial frontier. In the past, landmark case of Mohtarma Benazir Bhutto v President of Pakistan was a watershed moment. The Court decided that secret monitoring of telephone conversations was an unwarranted invasion of privacy and went beyond the idea of the privacy of home to include personal communication. This reasoning was futher updated by the apex court in Justice Qazi Faez Isa v President of Pakistan case, where the Court affirmed the constitutional right to privacy includes bank transactions and even the online footprint of an individual.

6.2 The "Subject to Law" Paradox and Legislative Reality

In spite of such broad judicial interpretations, the Subject to law provision of the Pakistani model is the major flaw. Although its intent was to permit the reasonable restriction, in effect, the privacy of a person in the cyber space does not fully enjoy constitutional protection but is instead constrained by evolving statutory frameworks.

Administrative emancipation of state power based on this clause has always been sought by courts:

- **Search Warrant Scrutiny:** In *Riaz v Station House Officer*, the Lahore High Court decided that a search warrant could not be obtained in a mechanical fashion which would violate the privacy guaranteed by the constitution.
- **Precedence over Criminal Investigation:** In *Zeeshan Ahmed v The State*, the court ruled that the investigation of a Hadd offence was inferior to the right to privacy and therefore warrantless raids were unconstitutional.
- **Mobile as Home:** The application of this jurisprudence in the case of Muhammad *Rahmat Ullah v The State*, has helped to understand that obtaining access to information stored in the mobile device of an individual without obtaining their consent, or without prior judicial authorization, is unlawful and unconstitutional. The court equated mobile phone with "home" as it contains the most private information of an individual.

However, the Article 14 in itself does not qualify as a data privacy model today, as it does not contain any substantive rules of processing data or consent, or penalties. This subjected the data of citizens to a state of legal insecurity, which the current statutory means are yet to address.

Section 7: Statutory Architecture: PECA 2016 as a Tool of State Control

The next striking fact is that the good laws on data protection in Pakistan do not exist: the major legislation that regulates the field of the digital world is the law on Prevention of the Electronic Crimes Act 2016 (PECA). PECA was also introduced keeping in mind the curtailment of electronic crimes but this turned out to be the primary instrument which was inappropriately employed in the matter of data abuse.

7.1 Criminalization over Protection: Individual Abuse vs. Corporate Accountability

Critical analysis of provisions and enactment of PECA, however suggests that it is more of a security and crime-control law which does not go the extra mile in ensuring that the right of persons in data privacy is not violated. According to this law, the most visible changes are premised on the principles of granting the states more power and criminalizing the actions of the individual where the rights-based approach will turn big and mighty data controllers into criminals.

PECA in its current form does have some protecting clauses. Sections 3, 4 and 5 criminalize the use of unauthorized access to, copying of, and interference with information systems and data. Section 16 expressly forbids the unauthorized use

of identity information of an individual. As a matter of fact, these provisions are not quite effective when it comes to systemic data protection. They are based on the demonstration of a criminal act committed by a person, and not on the failure of a platform. PECA case law, such as in Junaid Arshad v The State, generally involves the person being charged because of misusing the data of another, and no legal review is conducted against the platform where such misuse occurred. This individualist approach does not reflect on the contribution of corporations that store and process data at a very huge scale.

7.2 The Surveillance Mandate: Sections 32 and 38 as Barriers to Privacy

PECA clauses grossly encroach the privacy rights in the name of promoting state power. The most absurd is the section 32 which requires service providers to retain traffic data for one year or more. This law is the foundation of giant data storage, an action that violates the core concept of data protection, minimization. It grants access to state agencies to huge amount of data of citizens, therefore, encouraging mass surveillance.

The extensive coverage of the state-centric approach, the safe harbor provision, in section 38, " Limitation of liability of service providers. This is subject to the condition that, a service provider, would not be liable unless he has certain actual knowledge and, willful intention to knowingly and voluntarily participate in the breach of the act. In other words, this imposes a highly burdensome weight on claimants. It promotes willful blindness by platforms since the liability arises when the active and knowing participation is involved and not when they do not or fail to act. The example of the case of Careem, a ride-hailing firm in Pakistan, can be given in this regard. The company, Careem, did not held accountable in relation to its severe information breach in 2018, which comprised of the information of millions of Pakistani clients, is illustrative of the inefficiency of this provision, and the Act, on the whole.

7.3 The 2025 Amendment: From Data Protection to Content Surveillance

The PECA (Amendment) Act 2025 is a further departure from the principles of privacy and data protection, which shifts the legislative value towards the surveillance and control of communication content, as well as covering aspersions of the state institutions. The creation of the Social Media Protection and Regulatory Authority (SMPRA) to regulate the unlawful or offensive content and covering the aspersions of the state institutions in particular, it requires intrusive monitoring of communications, which further undermines the constitutional right to privacy.

There is no Data Protection Authority in this Act but the Cyber Crime Wing of the Federal Investigation Agency (FIA) is replaced with the National Cyber Crime Investigation Agency (NCCIA). Since the NCCIA is still an investigation agency and powers has been given to them to investigate, prosecute and arrest the individual for online speech violations. This will surely increase state surveillance of individuals thereby violating the constitutionally protected right of privacy.

Section 8: The Personal Data Protection Bill (PDPB) 2023/2025: A GDPR Clone?

The Personal Data Protection Bill (PDPB) can be considered a milestone in the history of digital rights in Pakistan and a changing of the course toward a more informational privacy and rights-centered approach instead of crime-control, which may enhance the trust demanded to build a flourishing digital economy.

The Objectives of the Bill Statement is categorically founded on the right of privacy in the Constitution of Pakistan and establishes the protection of data as a prerequisite to the informational privacy. Such a rights-based framework is certainly a departure from the old legal order, and an act of a new rights-oriented and citizen-focused one.

8.1 Imported Principles and the GDPR Blueprint

The PDPB reflects various fundamental principles of the European model in granting a set of enforceable rights to the data subjects. These are the Rights to Access, the Rights to Correction and the Rights to Erasure (commonly known as the

Right to be Forgotten). in addition, there is the Data Portability, which authorizes users to transfer their personal data between controllers in machine-readable form.

The Bill places systemic responsibilities on the data controllers in addition to the individual rights and outlines clear-cut rules for the entire data processing cycle. It requires data to be obtained for "specified, explicit and legitimate purposes" and must be "adequate, relevant, and limited" to those stipulated purposes (the principle of data minimization). In addition, it imposes rigorous security measures, sets data retention caps, and adds a critical requirement for personal data breach notifications, obligating controllers to notify both the National Cybersecurity Policy Development Board (NCPDP) and concerned data subjects within a 72-hour window upon a breach.

8.2 Localization and Cross-Border Transfers

The chapter VI of the Bill looks at the intricacies of the globalized data economy. It stipulates that the receiving country needs to have an "adequate personal data protection legal regime." Interestingly, it stipulates that "Critical Personal Data" is to be processed only in servers or digital infrastructure in Pakistan, resolving data localization issues for the most sensitive data. Although the bill allows transfers to countries with sufficiently legal frameworks, the conditions of national sovereignty and national security is there.

8.3 The "Independence Deficit": Executive Control vs. Autonomy

Under the guise of its rights-based terminology, however, the actual analysis of the matter shows that the NCPDP has a structural weakness of its kind since, despite the label of an autonomous body, this particular institution is under the administrative control of the Federal Government. The bill also provides the government with absolute authority in appointment and removal of members of the Commission, and make binding policy directives regarding the work of the authority. These provisions undermine the independence of the Commission which is virtually reduced to a part of executive. This means that the NCPDP might be reduced to a tool of government policy and not an independent enforcer of data rights of citizens.

Section 9: Emerging Digital Governance: AI Policies, Centralization, and Content Regulation

With the country progressing towards the digital transformation process, the data protection regulations are becoming even less aligned with the international practice. In contrast to the EU, where the regulatory ecosystem is developed and consists of the GDPR, AI Act, and Digital Markets Act (DMA), Pakistan is still concentrated on the more centralized strategy, where national security, state-led digitalization, and content regulation are prioritized.

9.1 Draft National AI Policy (2023/2024): Development vs. Risk Management

The Draft National Artificial Intelligence Policy is the first move of regulating the emerging technologies in the country; however, the philosophy underlying it is vastly different compared to the EU AI Act, since the Pakistani policy focuses on the creation of the socio-economic progress and ensuring the protection of the national security.

The draft policy is intended to incentivize the adoption of AI in key sectors of the economy including healthcare, financial, and agricultural to harness the potential of technologies to promote national development. This policy prioritize development over privacy risk management. It proposed that AI Regulatory Directorate (ARD) under the proposed National Commission of Personal Data Protection (NCPDP) should be established. However, NCPDP does not yet exist as the PDPB is yet to become law. So in the absence of regulatory authority, there are various risks, such as AI collecting massive amount of data, and also making biased decisions which violate the fundamental rights of individuals.

9.2 Digital Nation Pakistan Act (2024/2025): The Centralization Paradox

Digital Nation Pakistan Act, 2024 is seen as the antithesis of the EU Digital Markets Act (DMA). It focuses on the centralization of the digital ID and government data system is positioned as the

solution to a firm and resilient digital ecosystem that support innovation, connectivity and integration across different sectors.

On the other hand, legal analysts caution that this centralized architecture, without including user's rights and adequate provisions like Art 32 of GDPR, will constitute a single point of failure to privacy, exposing the entire national databank to state surveillance or unauthorized access, processing and deletion of data. In the absence of an active Personal Data Protection Act such centralization seems like a measure of "digital authoritarianism" and it means that anyone can process data and will be able to suppress dissent through AI-assisted monitoring.

Conclusion

This study has critically evaluated the changing data privacy legislation in the European Union and Pakistan and the results suggest that there is a huge gap between a rights-based regime, which operationalizes data privacy on a Gold Standard, and a developing security-based regime. By implementing the building block of Article 8 of the ECHR and lawmaking framework of the GDPR, the AI Act, DSA and the Digital Markets Act, the European Union has managed to enter into a holistic environment, where human dignity, institutional autonomy, and corporate responsibility are prioritized.

Instead, the Pakistani landscape is still typified by a Constitutional Mirage. Although Article 14(1) of the Constitution of 1973 gives an explicit pledge of sacred inviolable dignity and privacy, the right is always restricted by legislation via the subject to law paradox. The main regulatory act is the Prevention of Electronic Crimes Act (PECA) 2016, which is more of a state control measure and is focused on criminalization rather than providing a personal safety guaranty. The 2025 Amendment has further supported this security-first orientation and focused on content surveillance and monitoring of aspersions against state institutions rather than the genuine protection of the data of citizens.

The introduction of Personal Data Protection Bill (PDPB) 2023 and the Draft National AI Policy marks a historic shift in Pakistan. Although such efforts have tried to emulate GDPR-type concepts of minimizing data, purpose limitation, and giving the right to be forgotten, they are presently sabotaged by lack of an independent institution (suggested National Commission on Personal Data Protection) (NCPDP). The PDPB has not yet been passed by the parliament. On the other hand, the very structure of total executive control and delegation of enforcement by the law enforcement agencies with police powers, including the NCCIA, generate the basic conflict of interest threatening to make these new protections merely cosmetic.

Finally, for Pakistan to bridge the gap and reach the stage of adequate standard in line with the global standards, a paradigm shift is required. The Parliament should go further than the surveillance-by-design model and create an actual independent watchdog that could save citizens of the corporate exploitation and the state-sponsored overreach. Unless Pakistan commits to an institutional independence and shifts towards a rights-first form of digital rulebook, the constitutional promise of privacy in Pakistan will not be actualized in an increasingly data-driven world.

References

Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).

Constitution of Pakistan art 14(1).

Benazir Bhutto v Federation of Pakistan **PLD 1998 SC 388.**

Justice Qazi Faez Isa v Federation of Pakistan PLD 2021 SC 1.

Muhammad Hammad Amin and Maira Hassan, 'Digital Privacy in Pakistan: Ending the Era of Self-Regulation' (Shaikh Ahmad Hassan School of Law, 6 December 2021) https://sahsol.lums.edu.pk/node/17036 accessed 14 July 2025.

Aly H. Ul Haq, 'The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill' (2024) 2(2) UCP Journal of Law & Legal Education https://ojs.ucp.edu.pk/index.php/ucpjlle/article/view/122/147 accessed 1 December 2025

Areeba Iqbal Qureshi, 'AI and Privacy: A Paradox?' (SSRN, 2 August 2023) https://ssrn.com/abstract=4537749 accessed 5 January 2026.

Peter Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer 2017).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L2024/1689.

European Commission, 'AI Act' (Shaping Europe's digital future, Digital Strategy) https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai accessed 1 December 2025.

Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs 2019).

Constitution of the Islamic Republic of Pakistan, 1973, art 14(1): "dignity of man and, subject to law, the privacy of home, shall be inviolable".

Mohtarma Benazir Bhutto v President of Pakistan PLD 1998 SC 388; Justice Qazi Faez Isa v President of Pakistan PLD 2020 SC 1

Prevention of Electronic Crimes Act, 2016 (PECA), s 32 (Mandatory Data Retention).

Personal Data Protection Bill, 2023 (PDPB), s 34 (Exemptions) and s 43 (Policy Directions to Regulator).

ECHR, art 8(1).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector (Digital Markets Act) (2022) OJ L265/1.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on Artificial Intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2016/798 (Artificial Intelligence Act) [2024] OJ L, 2024/1689.

Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Schrems II) EU:C:2020:559

GDPR, art 4(1)

GDPR, art 5(1)(a): Personal data shall be: processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

ibid, art 5(1)(b): Personal data shall be: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

[1] ibid, art 5(1)(c). adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');

Ibid, art 25

ibid, art 5(1)(f): processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality').

ibid, art 15: Right of access by the data subject

ibid, art 16: Right of rectification by the data subject

ibid, art 18: The data subject shall have the right to obtain from the controller restriction of processing where certain condition applies.

ibid, art 20.

ibid, art 17: Right to erasure ('right to be forgotten')

Mario Costeja González EU:C: 2014:317 *and* Case C-131/12 *Google Spain SL v AEPD*

Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others (Joined Cases C-293/12 and C-594/12) [2014] ECLI:EU:C:2014:238.

Case C-203/15 Tele2 Sverige AB v Post- och telestyrelsen and Case C-698/15 Secretary of State for the Home Department v Watson and Others ECLI:EU:C:2016:970.

ibid

La Quadrature du Net, Federation of Non-profit Internet Service Providers, Franciliens.net, French Data Network v Prime Minister, Minister of Culture (Case C-470/21, ECLI:EU:C:2024:370)

Frances M Green, 'Adequacy of the EU–U.S. Data Privacy Framework Survives Challenge' (Workforce Bulletin,2 September 2025) https://www.workforcebulletin.com/adequacy-of-the-eu-u-s-data-privacy-framework-survives-challenge#:~:text=Conclusion,the%20preparation%20of%20this%20post. accessed 12 November 2025.

European Data Protection Board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (11 November 2020).

European Union Agency for Fundamental Rights (FRA), *GDPR experiences of data protection authorities* (2024).

ibid

GDPR, art 51: Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ('supervisory authority').

GDPR, art 52: Each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation.

Constitution of the Islamic Republic of Pakistan 1973, art 14(1).

Mohtarma Benazir Bhutto v President of Pakistan PLD 1998 SC 388.

Justice Qazi Faez Isa v President of Pakistan PLD 2021 SC 1.

Personal Data Protection Bill 2023, Statement of Objectives (Ministry of IT and Telecommunication, Government of Pakistan)

PDPB 2023, s 16: Right, to access.

ibid, s 19: Right to correction.

ibid, s 26: Right to erasure.

ibid, s 29: Right to data portability and automated processing.

Ibid, s 5(2): The personal data shall be collected for specified, explicit and legitimate purposes, which shall not be processed further that is incompatible with the aforementioned purposes and shall be adequate, relevant, and limited to the purposes for which the data is processed.

Ibid, s 9: Given the national interest, the Commission shall prescribe the best international standards to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration, or destruction.

Ibid, s 10: The personal data processed for any purpose shall not be kept longer than necessary for the fulfillment of that purpose or as required under the law

Ibid, s 13(1): (1) In the event of a personal data breach, the data controller shall without undue delay and where reasonably possible, not beyond 72 hours of becoming aware of the personal data breach, must notify the Commission and the data subject except where the breach

is unlikely to result in the infringement of rights and freedoms of the data subject.
Ibid, s 31(1): Condition for Cross border transfer.
Ibid, s 31(2).
Ibid, s 35(2): The Commission shall be an autonomous body under the administrative control of the Federal Government with its headquarters located in Islamabad.
Ibid, s 36(1) and s 37(2).
Ibid, s 43: Powers to issue policy directives.
Areeba Iqbal Qureshi, 'AI and Privacy: A Paradox?' (SSRN, 20 November 2023)
Nadir Guramani, *Digital Nation Pakistan Bill tabled in National Assembly* **Dawn (online)** (16 December 2024) https://www.dawn.com/news/1879138 accessed 7 January 2026.
GDPR, art 32: Security of processing
Huzaima Bukhari, Dr Ikramul Haq and Abdul Rauf Shakoori, '*Digital Nation Act: a critique*' **Business Recorder** (21 February 2025) https://www.brecorder.com/news/40349203 accessed 7 January 2026.