

Privacy in the Age of Surveillance: Reconciling State Security Interests with the Constitutional Right to Privacy in the Digital Era

Muhammad Babar Shaheen ^{1*} Muhammad Shahid Sultan ² Ahsin Ali ³

¹ Lecturer, College of Law, Government College University, Faisalabad, Punjab, Pakistan. Email: bsharal@yahoo.com

² Assistant Professor of Law, Government College University, Faisalabad, Punjab, Pakistan. Email: shahid6023@yahoo.com

³ Lecturer, Department of Law, University of Sahiwal, Sahiwal, Punjab, Pakistan. Email: ahsin.ali@uosahiwal.edu.pk

ABSTRACT: Digital surveillance has become a routine feature of governance, policing, intelligence, border control, welfare administration, and platform regulation. Its constitutional significance lies not merely in the quantity of data collected but in the capacity to combine communications content, metadata, location histories, biometric identifiers, device information, and algorithmic inferences into persistent profiles of individuals and groups. Pakistan faces a genuine security environment involving terrorism, violent extremism, espionage, organized crime, cyberattacks, and threats to critical infrastructure. Nevertheless, national security cannot convert secret technological capacity into legally unreviewable power. This paper examines how Pakistan can reconcile legitimate state-security interests with the constitutional right to privacy in the digital era. Using a doctrinal and comparative method, it interprets Articles 4, 8, 9, 10A, 14, 19, and 19A of the Constitution alongside Pakistan's interception, telecommunications, cybercrime, digital-governance, and proposed data-protection frameworks. It then compares Pakistan with India, the United Kingdom and European human-rights system, the United States, and Canada. The paper argues that Article 14 must protect informational and communicational privacy beyond the physical home and that any surveillance measure must satisfy legality, legitimate aim, evidence-based necessity, strict proportionality, independent prior authorization, minimization, secure retention, accountable sharing, and effective remedy. The 2024 Islamabad High Court proceedings concerning the Lawful Intercept Management System and Amnesty International's 2025 investigation illustrate the consequences of allowing infrastructure to outpace law. The paper proposes a Pakistan-specific model combining judicial authorization, specialized independent oversight, privacy-by-design, delayed notification, transparency reporting, and comprehensive data-protection legislation. Properly designed safeguards do not obstruct security; they improve intelligence quality, institutional legitimacy, evidentiary reliability, and constitutional trust.

KEYWORDS: Privacy Surveillance, National Security, Article 14, Digital Constitutionalism, Data Protection, Interception, Proportionality, Artificial Intelligence

Introduction

The issue of surveillance that was discussed in the Constitution has evolved in both scope and type. The usual surveillance in the past was that the state would have to pursue a specific individual, visit a specified area, wiretap a

Pages: 300 – 317

Volume: 5

Issue: 5 (May 2026)

Corresponding Author

Muhammad Babar Shaheen

✉ bsharal@yahoo.com

Cite this Article: Shaheen, M. B., Sultan, M. S., & Ali, A. (2026). Privacy in the Age of Surveillance: Reconciling State Security Interests with the Constitutional Right to Privacy in the Digital Era. *The Regional Tribune*, 5(5), 301-317.

<https://doi.org/10.55737/trt/v-v.293>

specified line or get a specific set of records. Digital systems reduce the cost of observation, move it to ongoing and retrospective and also make it searchable. Mobile networks show how mobile people move; platform systems store communications and behavioural patterns; biometric systems link bodies to the state database, and even AI can deduce characteristics that people have never explicitly given (Wachter & Mittelstadt, 2019). When combined, analysed, and presented, a disjointed set of mundane facts can thus be a close-up of a portrait. Contemporary privacy scholarship thus views privacy as a state of autonomy, dignity, democracy and freedom from domination, not as a limited pursuit of privacy and secrecy (Tabassam & Hussain, 2024; Citron, 2022; Hildebrandt, 2020; Véliz, 2020).

They are also monitoring those who are never prosecuted. When people know they might be listened to, they behave differently; they don't associate; it undermines the ability to report confidentially; it puts lawyers and their clients in danger; and it can put people's political views at risk (Tufekci, 2017). The damage is thus more structural in that the power of observation is shifted away from the citizen to institutions that can collect, interpret and act on data on a pervasive basis. According to Lyon (2018), this is a culture in which watching is normalised, and according to Zuboff (2019) it is a culture of behavioural extraction which draws economic and political leverage. The use of large databases can, in policing, turn suspicion into a statistically based classification, and this can be an institutional bias (Brayne, 2021; Ferguson, 2017). These concerns are especially salient in countries with opaque intelligence mandates, in terms of independence of regulatory institutions, and in terms of getting remedies.

In order to be able to respond, Pakistan has to deny the security interest. Terrorist attacks have been ongoing in the country, as well as militant attacks, sectarian attacks, espionage, cybercrime and attacks on public institutions. Where the state is doing more than merely protecting life, it can use interception, data retention, tracking location or covert access of a specific individual where there is a serious and demonstrable threat. That is not the question of whether surveillance can ever be used; it's whether it's the right thing to be used. It is about the extent of surveillance that is legal and strictly defined by law, whether an independent authority has the necessary confidence that it is warranted, the proportionate nature of the technique, scope, duration and type of data being collected, and whether there are independent and effective safeguards to ensure that the data collected is kept under control throughout its life cycle. However, international human-rights bodies have become more vocal than ever about the need to review the legality of surveillance at each of its stages, as it becomes more intrusive at each point (European Court of Human Rights [ECtHR] & European Union Agency for Fundamental Rights [FRA], 2025; Human Rights Council, 2021; Office of the United Nations High Commissioner for Human Rights [OHCHR], 2018, 2025).

The institutions are not as strong as the constitutional structure of Pakistan. The dignity of a person and the inviolability of his home (subject to law) are declared by Article 14 (National Assembly of Pakistan, 2025). Articles 4 and 8, 9 and 10A, and 19 and 19A are continuity and support to the themes of lawful treatment/constitutional supremacy, liberty, and fair process, and to expression and access to information, respectively. In the case of Justice Qazi Faez Isa v. President of Pakistan (2021), the Supreme Court related privacy with autonomy, human dignity and democratic freedom, and decried the covert action of the state without any law and due process. The judgment of the Court, while reviewing the Violation of Fundamental Rights case, also reiterated that the Constitution does not distinguish between the person targeted or not (Justice Qazi Faez Isa v. President of Pakistan, 2022). Combined, these authorities provide an information-based understanding of privacy that extends beyond the doorstep of the home, into digital communications (Butt et al., 2024).

The major issue is that there is little integration. Cyber-related offences, data preservation and investigation and access to data are regulated by the Prevention of Electronic Crimes Act 2016 (PECA), with a warrant structure for specified forms of surveillance provided in the Investigation for Fair Trial Act 2013, while the Prevention of Electronic Crimes (Amendment) Act 2025 introduced a number of changes to the institutions and offences that

govern online activity, including telecommunications legislation. The Digital Nation Pakistan Act 2025 (which was not enacted into law as of August 2026) introduced a comprehensive digital-governance framework, and the proposed Personal Data Protection Bill 2023 has yet to be passed into law (Chambers & Partners, 2026; DLA Piper, 2026; International Comparative Legal Guides [ICLG], 2026). The state is therefore laying the groundwork for infrastructure to be more digitally integrated, rather than rights. So the state is constructing a more digitally integrated infrastructure before developing a more integrated rights regime.

The Islamabad High Court's decision in W.P. is a testament to the urgent need for the matter to be resolved. No. 2758/2023. On the material that has been placed before it, the Court stated that telecommunications operators had been instructed to implement a Lawful Intercept Management System (LIMS); that designated agencies have access to communications and metadata; and that the technical capacity is capable of accessing around two per cent of its subscribers at any one time. The Court rendered its findings with a preliminary nature, but there were serious issues about the authority, supervision and compliance of the legislation raised by it (Islamabad High Court, 2024). In its later investigation, Amnesty International found that in addition to the surveillance and censorship that were already documented, there was a wider surveillance and censorship ecosystem composed of LIMS and web-monitoring infrastructure and that procurement, technical deployment, and protective measures were opaque (Amnesty International, 2025). These materials do not establish that all capabilities are exercised against all citizens; they illustrate the need for constitutionally supervised exercise of capacity itself.

This paper seeks to make the case for structured reconciliation, instead of rhetorical balancing. National security is a political issue, but one that has to be defined by constitutional requirements which can be subject to legal review. There are no absolute rights to privacy because it isn't absolute. The right model is one of limited capacity: the state can implement technically effective measures only when it is lawfully prescribed, evidence is legally authorized, invasion of the collateral is minimized, oversight of the data occurs, and the remedy that is applied corrects the abuse. Comparative law shows that the detail of the procedures without independent institutions can become formalistic, and the absence of these institutions from constitutional recognition is weak. Pakistan requires both.

Research Questions, Scope, and Method

The research consists of four questions. First, what does Article 14 mean in the light of private life accessed via telecommunications networks, cloud services, biometric databases and interoperable government platforms? Second, whether the current surveillance and data-governance framework in Pakistan meets the legality, necessity, proportionality, independent oversight and effective-remedy criteria. Third, what lessons are learned from India, the United Kingdom and the human-rights system of Europe, the United States, and Canada. Fourth, what changes to the laws and institutions would ensure that the security in the operation would not be breached in any way, without giving rise to arbitrary or politically motivated surveillance.

It is a doctrinal, comparative and normative approach. The doctrinal analysis does not merely look at the words 'privacy of home' as it is found in the Constitution, but rather takes a holistic view of the Constitution. It explores judgements by judicial bodies in Pakistan, laws passed by official bodies, combined laws, policy documents and reports by institutions during recent years. The comparative analysis is practical in that it does not presume that foreign rules can simply be imported without any modification, but rather explores how the foreign systems deal with the issue of authorization, the collection of bulk data, metadata, oversight, notification, remedies, and data protection. The normative analysis, which considers these rules in the context of a rights-protective security

framework based on legality, necessity, proportionality and accountability, follows Bhatia (2019); Kuner et al. (2020); OHCHR (2018); and OHCHR (2025).

The bibliography has been limited to a specific time frame because of the timeframe of the study (2016-2026). The older Pakistani acts which continue to be in force are discussed in the context of the present official consolidated texts consulted in 2026, numbering the entry according to the year the text was consulted, not on the year the Act was passed. Only academic sources from 2016 are used. This strategy allows for engagement with the core legal framework, and also helps keep the scholarship, comparative jurisprudence, policy reports and empirical data up to date with the digital world.

Development of a Code of Practice for Privacy in the Digital Pakistan Context

The right to privacy in Article 14 should be understood as a right to the dignity of privacy, and not a rule that is just for physical premises. The home is a special place that is singled out, but the reference to human dignity is more general. Digital communication is now used for tasks traditionally believed to be domestic: personal communication, family life, professional advice and consultation, political organization, religious observance, financial management and personal record keeping. A spatial reading would give rise to an irrational consequence: a private letter kept in a desk is secure while the same letter kept on a phone and/or server is constitutionally exposed. More recent constitutional studies have been interested in measuring the degree of control, inference, vulnerability and power that the processing of data can create, rather than indulging in technological formalism (Cohen, 2019; Hildebrandt, 2020; Hussain et al., 2026).

The decision of the Supreme Court in Justice Qazi Faez Isa v. President of Pakistan (2021) is at the heart of the matter. The case was related to the illegal collection and utilization of information on a sitting judge and his family. The judgments were connected to personal agency, dignity and the capacity of citizens and institutions to operate in a free and uncoerced way, and to privacy. But surveillance was not something to be treated as a minor error in procedure; it was known to be a power that could shape public life and jeopardise the independence of the judiciary. In the 2022 review decision, the due process was upheld, and the idea that the state can go around the constitutional protections because it has an accountability objective was rejected (Justice Qazi Faez Isa v. President of Pakistan, 2022). The three propositions these decisions support are: surveillance is interference even before the information is made public; legality goes beyond administrative convenience; and constitutional review should take into account institutions, their methods, and purpose.

Article 9 further supports this reading as it adds the concept of freedom from 'unjustified tracking, profiling and coercive inference' to those listed above. In Pakistan, the concept of life has been interpreted as a much broader one than just physical life from the time of inception of the Constitution. In the digital world, somebody whose whereabouts, associates, reading patterns and communications are always known to the State could have freedom of movement but not freedom of action. Comparative constitutional courts have also undergone a change. The Indian Supreme Court had a broader definition of privacy, which included protection of bodily integrity, decisional autonomy, informational self-determination, and development of personality (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017). Canada's Supreme Court has also made clear that the use of digital identifiers can give insight into a person's biography and establish reasonable expectations of privacy even when data is in the custody of intermediaries (R. v. Bykovets, 2024).

The principle of Article 4 is that "every person shall be treated according to the law." In surveillance cases, this has to be a substantive, not a ceremonial, principle. A secret policy or licensing condition, verbal instruction or an internal standard operating procedure is not a substitute for a law that sets out the powers and confines discretion.

Legal accessibility in intelligence is challenging, but the key principles are available to the public, such as types of offences, who decides, what the evidence needs to be, the maximum length, how privileged material is treated, how much is kept, who oversees the intelligence and what can be done about it. The ECtHR's contemporary approach to surveillance law also calls for the clarity of the law on the scope of discretion and how it will be exercised, and on end-to-end protection against abuse (*Big Brother Watch and Others v. United Kingdom*, 2021; *Centrum för Rättvisa v. Sweden*, 2021).

Article 8 invalidates any law which contradicts fundamental rights, to the extent of the contradiction. This does not mean that Parliament was able to somehow 'bury' the notion of security and public order within the broad language of its statute and thus render it immune from constitutional challenge. An exception to the right to surveillance should be interpreted restrictively or struck down if it allows for indiscriminate collection, doesn't require an independent authorization, and doesn't include restrictions on examination and dissemination. A rational method is proportionality in which the State must have a legitimate objective, be able to show a rational link between the measure and the objective, the latter must show that no less rights-restrictive but equally effective alternative measure is reasonably available, and the State must show that the public benefit justifies the rights harm (Bhatia, 2019; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

When surveillance material is used in criminal, administrative, tax or disciplinary proceedings, then Article 10A comes into play. It is appropriate to use secret evidence in a few limited national-security situations, but if collection methods are kept secret, the individual can be unable to bring authentic evidence, context, lawfulness or chain of custody to trial. If a lawful system cannot be tested, then it must be excluded or provide a redacted summary or disclosure, or use a special advocate or allow the judge to inspect it without any restrictions. Information gathered for the purpose of intelligence cannot be assumed to be for use in prosecution without re-evaluating the information under a new set of legal criteria. Intelligence and evidence can't be turned into a smoke-screen to skirt constitutional protections.

Pakistan's Surveillance and Data-Governance Framework

Pakistan's legal framework has several avenues for the authorities to gain access to and control over digital information. PECA 2016 establishes new offences for unauthorised access, interference, 'cyber-terrorism', identity information and electronic fraud and offers the preservation, search, and seizure of traffic data (Pakistan Code, 2026b). There is a need for some investigative powers as cybercrime is technically complex and can be very fast-disappearing evidence. The constitutional concern will be when the preservation and access orders are general and/or national security or public order are not defined, when data must be held by the service providers or when they can not challenge the collection of data. However, the duty of interpreting PECA cannot be confined to the concept of a security code on its own, but is subject to the interpretations of Article 4, Article 9, Article 10A, Article 14 and Article 19 (Daudpota, 2023; Haq, 2024; Munir, 2025; Rana & Iqbal, 2025).

The Prevention of Electronic Crimes (Amendment) Act 2025 has been passed to widen the scope of institutions overseeing online content and cybercrime and added a crime around false or fake information. The amendments were brought into the system to react to harmful online activity, harassment, and disinformation. The vague language and influence of the executive and speedy removal processes could lead to censorship and selective enforcement, critics said (Human Rights Watch, 2025; Kaye, 2019; Wajahat et al., 2025). Content regulation and surveillance are distinct concepts in law, but intermingle in the context of enforcement of content regulation, where the need for user identification, retention of records of platform use, network monitoring and analysis of political speech all are

relevant. Such a law can thus be used to extend the scope of surveillance—unless access to user data is separately provided and strictly limited to a serious crime.

The Investigation for Fair Trial Act has a judicial-warrant system for current investigation methods with regard to scheduled offences. It's important because of the recognition that there needs to be a covert surveillance mechanism not just in the executive but also as a mechanism that is initiated by the executive. However, the Islamabad High Court trial shows that there is a significant gap in implementation. The Court was apprised that for a long period, agencies have not been relying on the warrant process; rather, they have had access to the technical process through other means (Islamabad High Court, 2024). If all they are seeking is the same or greater data, or the same or greater access to it using telecommunications licensing, informal requests or standing network interfaces, a warrant law is of little constitutional value. The law should include an exclusivity provision, that is, where monitoring is considered to be under the ambit of the law, no alternative administrative process can circumvent the protections of the law.

The power to intercept is provided in the context of national security or offences in telecommunications law; but this is very broad, and must be tempered with the later warrant-based framework and the Constitution (Pakistan Code, 2026a). The present collective texts are not to be interpreted as a permission to access any networks in general and permanently. A power that enables a particular interception is distinct from a power that enables unidentified agencies to pick their targets without getting approval from an outside power at the time of the interception. The Islamabad High Court's preliminary order on LIMS serves as a good example to this end. The Court noted that the operators had no idea of the targets they were selecting and that information could consist of call data, messages, content, and web records (Islamabad High Court, 2024). The existence of a technical interface does not in and of itself constitute a violation of the law, but each and every use is required to have a legitimate authorization, technical restraints, audit logs and independent review.

The LIMS litigation is uniquely significant, as it brings the focus to system architecture, instead of the warrant document. A traditional model would involve approving a target by a court, and the provider would follow through on a limited request. Under such a direct-access model, an agency could communicate to the network via an interface, and wouldn't always be able to know it was legal or if it was being overreached. Formally protective measures, therefore, can be overcome by architecture. A rights-compliant system would need to have a digitally signed warrant, have to be validated at the selector level, automatically expire, have to be authorized at multiple levels of access, have to have immutable logs, and alert when access goes beyond what is warranted. Oversight bodies need to be able to determine who was asking, who is answering, when, why, for what legal reason, what data was returned and whether or not the data was subsequently shared or deleted.

This report brings a transnational element to the story, from Amnesty International (2025). It revealed that Pakistan had technologies and companies from various jurisdictions that facilitated its surveillance and censorship operations, as well as infrastructure linked with web monitoring, deep-packet inspection and interception. These are just some of the examples that make procurement a constitutional phase. A review of human rights can only start after a system is put in place. Questions that public authorities should ask themselves are whether the technology is used for indiscriminate collection, whether the audit function is incorporated, whether foreign vendors can still be accessed, and whether updates are made to the technology, which would add new capabilities, as well as whether supply contracts can be inspected or suspended (Amnesty International, 2025). Companies that provide surveillance technology also have human rights obligations to do human rights due diligence as well as to prevent foreseeable abuses (Deibert, 2020).

The lack of a comprehensive law in Pakistan which has been enacted to protect data only adds to these risks (Privacy International, 2017). PECA contains some provisions on lawful grounds for the processing, on limitation of purpose, on data minimization, on access rights, on rights to correction and erasure, on breach notification, on independent supervision and on administrative remedies, but lacks a comprehensive framework in these areas. The Personal Data Protection Bill 2023 would take Pakistan a step closer to a general framework, though analyses have derided loopholes in the bill, including general exceptions by the government, localization clauses, the lack of regulatory autonomy, and the lack of clarity with respect to cross-border transfers (Daudpota, 2023; Greenleaf, 2021; Haq, 2024; International Bar Association, 2025). According to Chambers and Partners, DLA Piper and ICLG, as of August 2026, there are still no comprehensive guides available to the bill as it becomes an enforceable statute.

The Digital Nation Pakistan Act 2025 provides an opportunity for service delivery, interoperability and administrative efficiency, but also heightens the impact of laws that are ineffective in providing privacy protection. Pakistan Digital Authority (2026) talks about a National Architecture that includes Data Exchange, Digital Public Infrastructure, and AI Governance. Interoperability minimizes duplication, but can also break down contextual barriers between the different areas of taxation, health, education, policing, welfare and identity. Information provided for a specific purpose may be made available for other purposes without substantial warning and consent. Consent is not enough of a protection in compulsory public services; instead, the following factors must be considered: statutory purpose, necessity, access controls, and independent supervision (Cohen, 2019; Kuner et al., 2020).

Biometric identities require special protection as they may be irretrievably compromised. While fingerprints, facial templates, iris patterns and family relationships are not changeable, you can change the password. Biometric databases can help to enhance authentication and stop fraud; however, the same databases can be used in a manner that results in the tracking of individuals. Authentication and fraud reduction are some of the benefits of biometric databases, but it is possible for them to evolve into tracking. In public places, facial recognition could be used to compare all the people that pass by with watchlists, leading to suspicionless screening on a population scale. Women, minorities and those who are not well-represented in training data can be especially affected by algorithmic error. Human review is an ineffective remedy in a system where the operators rely on the automated output or affected individuals can't challenge the match (Binns, 2018; Mantelero, 2022; Mittelstadt et al., 2016; Selbst et al., 2019; Wachter et al., 2021).

There is also a relationship between the private sector and the state with regard to surveillance. Telecommunications operators, social-media companies, banks, transport companies, and data brokers are sources of information that could be of interest to government officials. In the constitutional analysis, it is important not to presume a loss of protection for information when it is released to a service provider (Solove & Schwartz, 2020). That sort of disclosure is essential to digital participation; frequently, if there were any alternatives, they wouldn't work. *Carpenter v. United States* (2018) has denied that there is a categorical exception to the ECHR's third-party rule for historical location information, while *R. v. Bykovets* (2024) has upheld privacy in IP-address information as it could lead to detailed information about one's online activity. The same approach is to be considered for Pakistan as well, where the idea that provider-held data is 'abandoned' should not be the rule.

Protection is not an abstract concept but has practical consequences. Digital Rights Foundation (2025) reported that thousands of complaints have been made in Pakistan regarding privacy violations, including harassment, impersonation, non-consensual intimate images and account compromise, both by the state and private entities.

Other restrictions and arrests, concerns regarding surveillance, and self-censorship were also noted by Freedom House (2025), the Human Rights Commission of Pakistan [HRCPP] (2025), and Human Rights Watch (2026). All these sources should be taken with a grain of salt as they reflect the use of different methodologies and approaches to normativization, but all of them demonstrate that the goal of the privacy reform must be to ensure citizens' security against crime, while at the same time preventing the extension of enforcement powers as a new source of insecurity.

Problems with the Current Model in the Constitution

The first defect is that it is not clear if it is legal. Surveillance rules are found in a variety of statutes, licenses, regulations, standard operating procedures, procurement arrangements and institutional practice. It's not reasonable to expect any citizen to know what categories of data any agency might have access to, or that any threshold might exist. The legal framework can't be secret, but any other operational details could be kept confidential. The necessary conditions of surveillance need to be adopted by Parliament and be public. The ECtHR has consistently found that foresight does not have to be about when surveillance will take place; it involves law limiting discretion and its potential arbitrariness (*Big Brother Watch and Others v. United Kingdom*, 2021; *Centrum för Rättvisa v. Sweden*, 2021).

The second defect is the type of concentration which is under the control of the executive. If the same institution is responsible for detecting the threat, deciding on the target, approving the technique, gaining access to the data, interpreting the outcome and then reviewing compliance, errors and abuse are hard to detect (European Union Agency for Fundamental Rights, 2017). Authorisation by a Judge is not absolute; rather, it differentiates between investigation and approval and makes sure that an evidential record is kept. The authorizing judge should be provided with all the information, such as what factors pose a challenge to the application, proposed selectors, what should be collected as collateral, and handling of privileged communications. There might be an emergency access that can be allowed for an immediate threat to life, but should be terminated quickly otherwise, unless there is independent verification.

The third fault is that the parts are not sufficiently differentiated. All data and techniques aren't the same when it comes to intrusion. A query for a subscriber's name is not months of location history, a communication is not a complete device extraction, and targeted interception is not bulk acquisition. The law should put in place progressive levels. The most intrusive methods, such as hacking devices, tracking over time, biometric identification in public places, bulk interception, and access to journalists' or lawyers' communications, should have the highest evidential and institutional protections (Citron, 2022; Gellert, 2020; OHCHR, 2021).

The fourth fault is that the metadata is less sensitive. Metadata can be used to identify the parties, their location, contact time, duration of contact and frequency of contact. It reveals many aspects of a person's social sphere, religion, health, politics, and private life, over time. The Court of Justice of the European Union has invalidated general and indiscriminate retention of traffic and location data, which is only allowed if there is a 'serious and genuine threat' in the national security sphere (Commissioner of An Garda Síochána, 2022; *La Quadrature du Net*, 2020; *SpaceNet AG*, 2022; *Tele2 Sverige AB*, 2016). It is advisable that Pakistan's metadata should be based on its inferential power instead of its label.

One of the fifth and last defects is "Lifecycle Blindness. All subsequent uses don't necessarily follow from a valid collection decision. Data can be duplicated, expanded for other use, or analyzed for new purposes, and be shared with other agencies or stored long after the threat has passed. Modern data-protection law is based on purpose limitation, minimization, storage limitation, integrity and accountability – all of which require protection at the

point of bulk interception, which Big Brother Watch demands (EU, 2016a; Kuner et al, 2020). The law in Pakistan should differentiate between the collection, automatic filtering, manual filtering, dissemination, use for evidence and deletion and have a legal basis for each of these steps.

Weak remedy is the 6th defect. When everyone knows that the state is secretly monitoring you, which is what this is, there's a constant issue: that person cannot dispute that the state is spying on him. A remedy system should provide for complaints to be directed to a special tribunal and should give the tribunal powers to order deletion, compensation, discipline or systemic reform, with access to classified information and be empowered to appoint an independent counsel. In most cases, delayed notification should take place after the operational risk is over. A judge may be able to delay notification, but it should not be automatic; it should be perpetual secrecy. Remedies are more than for victims – they create jurisprudence and institutional learning.

Comparative Constitutional and Regulatory Lessons

Comparative experience does not create a model – it does create a list of safeguards and failures that seem to be recurring. An important Indian aspect is that the country has no general privacy provision in its Constitution, and the Supreme Court in Justice K.S. Puttaswamy (Retd.) vs Union of India (2017) declared privacy as a fundamental right of the Indian people. The Court's foundation for privacy was dignity, liberty, autonomy and various constitutional rights. It also provided a statement of the law, of a legitimate aim and of proportionality as restrictions on state interference. The ruling is persuasive for Pakistan as dignity is specifically mentioned as one of the rights protected under Article 14, which further provides a textual basis to Pakistani courts for information privacy.

The case of Aadhaar proves the strength and scope of judicial recognition, and so does the case of Ayodhya. The Ayodhya case is no exception to the power and scope of judicial recognition, as is the case of Aadhaar. In the judgment in 2018, the Indian Supreme Court confirmed most of the biometric identity programme, but struck down and/or limited some of its applications (Justice K.S. Puttaswamy (Aadhaar) v. Union of India, 2018). Most talked about the welfare delivery and authentication benefits, and the dissenting reason talked about surveillance, exclusion and architecture which might enable profiling. Khera (2019) reports on practical issues of authentication problems and centralization of identity data. The Pakistan lesson is that the declared goals of a digital ID are not the only criterion; it must also be designed inclusively, auditable, and linked to other databases, while offering non-digital alternatives.

This is only one more instance of judicial duty in relation to secrecy in India, in Pegasus. The Supreme Court gave a 'national security' response the brush-off when it held that this was inadequate and ordered the setting up of a technical committee under the chairmanship of a retired judge (Manohar Lal Sharma v. Union of India, 2021) after taking cognizance of allegations that spying had targeted journalists, politicians and others. The Court was aware that national security might justify the withholding of information, but that would not preclude judicial review. In Pakistan, where the courts don't have technical knowledge, they can have independent experts who can go and check systems, keep classified information and report back on the legality of systems, targeting, and safeguards.

The rights and obligations of digital personal data came into existence under the Digital Personal Data Protection Act, 2023 (DPDP Act) and Rules, 2025 (DPDP Rules); and the implementation was ongoing with the establishment of the Data Protection Board in 2026. However, there is opposition with respect to government exemptions as well as executive control (Digital Personal Data Protection Act, 2023; Digital Personal Data Protection Rules, 2025; Ministry of Electronics and Information Technology, 2026). It is time for Pakistan to learn the good practices and

lessons from its enactment and criticism. A general exception for intelligence and law enforcement agencies could allow law enforcement to control the processing of the more coercive, but not under effective control.

The Investigatory Powers Act 2016 (as amended in 2024) provides a detailed statutory definition of the powers of the U.K. Many warrants in the system are 'double locked' - first with an authorization granted by a Secretary of State, and then an approval granted by a Judicial Commissioner. It also introduces a special tribunal and an investigatory powers commissioner's office. This model demonstrates how national security can be under the control of the executive and independently ratified and continuously monitored by the legal system. Systematic auditing, error reporting and public explanation have been shown to benefit the Investigatory Powers Office through the 2024 annual report of the Investigatory Powers Commissioner published in 2025, which did not reveal targets for the Investigatory Powers Office to operate against (Investigatory Powers (Amendment) Act, 2024; Investigatory Powers Act, 2016; Investigatory Powers Commissioner's Office, 2025).

The UK model is not necessarily a best practice model. It's complicated, allows for bulk power and has been the subject of ongoing litigation. In *Big Brother Watch and Others v. United Kingdom* (2021), the Grand Chamber agreed that bulk interception does not run afoul of the European Convention, but did impose strict requirements on the need for end-to-end protection, separate authorisation, control over selectors and search terms, monitoring and review. The whole system of signals intelligence in *Centrum för Rättvisa v. Sweden* (2021) has been reviewed by the Court. These judgments are significant for Pakistan as they come after the first warrant. A regime of interceptions may be illegitimate even if a formal basis exists for their collection if there is a lack of control in their selection, examination, retention or sharing.

In the European Union, the rules on the retention of information are more stringent concerning the retention of information in a general manner. *Tele2 Sverige AB* (2016) refused to generally and indiscriminately retain traffic and location data for the purpose of combating crime. The necessity principle applies to national security in the event of an actual and imminent or likely threat, and is always subject to time limits, review and necessity, according to *Privacy International* (2020) and *La Quadrature du Net* (2020). Commissioner of An Garda Síochána (2022) and *SpaceNet AG* (2022) reiterated the need for the retention of broad files not to become the norm. But the key lesson isn't that it is impossible to ever use a big data set for security purposes; it's that general retention isn't something that should be treated as just the business of administering a data set.

A distinction which can be found in both the General Data Processing Regulation and the Law Enforcement Directive of 2016 is helpful. There are two different rights regimes: one for competent authorities processing data for law enforcement and another for ordinary public and private processing (EU, 2016a, 2016b). Similarly, Pakistan should not go overboard and provide a blanket exemption (European Data Protection Board, 2021). Intelligence and policing might need some specific rules, but specific rules must be even more stringent in coercive access areas, not devoid of rights.

The Convention 108+ (Council of Europe, 2018), which is the modernised version of the Convention 108, has highlighted the principles of lawful and fair processing, proportionality, transparency, data quality and security, independent supervisory authorities, and restrictions which respect the essence of rights. Other OECD principles of democracy that are mentioned in the OECD (2022) declaration on government access to private-sector data include: legal bases, legitimate aims, approvals, handling safeguards, transparency, oversight, and redress. The instruments take particular care of cross-border digital services and the part played by private intermediaries, which are very relevant for Pakistan.

The United States offers a more limited constitutional framework based on the Fourth Amendment, but recent cases recognize that digital scale is a changing environment that impacts privacy. Acquisition of historical cell-site location information was a search even when the information was kept by a service provider, the Supreme Court ruled in *Carpenter v. United States* (2018). The court's ruling was "deliberately narrow," but one that did not apply the third-party doctrine mechanically (Kerr, 2018). Similarly, in *Naperville Smart Meter Awareness v. City of Naperville* (2018), granular electricity data was identified as a means to detect activities inside of a home.

There continues to be disagreement in the lower courts regarding extended technological surveillance in the United States. Leaders of a *Beautiful Struggle v. Baltimore Police Department* (2021) considered an aerial-surveillance programme that could reconstruct movements as constitutionally significant, and *United States v. Tuggle* (2021) introduced new doctrine to allow for long-term pole camera surveillance, but recognised the implications of aggregation. The Supreme Court gave divided opinions in the *United States v. Moore-Bush* case (2022) regarding continuous home surveillance. A more direct proportionality test is advocated by the dignity language in Article 14, which allows Pakistan not to adopt the US expectation-of-privacy test as a whole. These cases, however, show that, by using duration, automation, aggregation, and retrospective search, it is possible to make observations that are publicly visible at any given time into an intrusive record.

Specialized institutions are also vital and constrained in intelligence oversight of the United States. The 2023 report by the Privacy and Civil Liberties Oversight Board on Section 702 included a section on targeting, querying, compliance incidents and proposed reforms, and the 2024 reauthorization bill included provisions that would further change some of the powers but would keep many the same (Privacy and Civil Liberties Oversight Board, 2023; Reforming Intelligence and Securing America Act, 2024). The lesson here is that periodic public reporting and institutional review are essential, but that non-independence, lack of access, lack of resources and weak recommendations are not.

Canada has a rights-based approach to digital information. In *R. v. Jarvis* (2019), the Court did not accept a purely spatial interpretation of privacy for the purposes of recording, but instead stressed the "totality of circumstances." The *R. v. Bykovets* (2024) case established that an IP address does carry the reasonable expectation of a user's privacy, as it can be linked to other information to determine a user's online activities. Canadian jurisprudence therefore takes the view that 'gateway' data exists – a seemingly minimal identifier can lead to the acquisition of a much more extensive informational profile. When an agency seeks an IP address, subscribers, device identification or records of where a device has been located, Pakistan's warrant thresholds should take into account this concept.

Finally, comparative law is based on ten key elements: public and precise law; independent prior authorization; serious and defined objectives; differentiation of thresholds; selector and duration limits; protection of privileged and sensitive data; logging and inspection; controlled sharing; delayed notification in line with possibilities; and effective remedies. There is disagreement between systems on whether there is any point at which there is proportionality in bulk surveillance. For Pakistan, this is not an abstract question which must be addressed. It should start with the assumption that indiscriminate collection is not justified and that the government must establish a justification for using less intrusive and targeted methods of collection if it wishes to do so.

A Structured Reconciliation Test and Reform Agenda for Pakistan

For Pakistan, it would be better to put in place a constitutional test for all manner of state access to personal data. Legal: Surveillance should be legally authorized by clearly written laws which specify the agencies to be responsible

for it, the purposes for it, the types of data that are subject to it, how it will be done, how long it will be conducted for, how it will be supervised, and what remedies will be provided for it. Executive rules can't give new powers of surveillance to the police.

The second criterion is a valid goal. There are legitimate reasons for surveillance in the cases of national security, protection of life, prevention of terrorism, serious crime and cybersecurity. But “to protect the government's reputation”, “to discourage criticism” or “to keep track of legitimate political debate” are too broad goals to grant the government a right to interfere.

Third, surveillance should have the characteristics of necessity and evidence-based justification. Authorities must have reasonable grounds, explain how the target is related to the threat, and explain why the less intrusive options are not adequate. General information gathering should not be allowed unless for a specific purpose or reason.

Fourth, measures need to have rigorous proportionality requirements. There are several factors that should be taken into account when making a decision – the seriousness of the threat, sensitivity of data, number of individuals impacted, length of time, potential risks of misuse and harm to democratic participation. Security measures can be illegal if they are gathering too much or too irrelevant information.

Fifth, the use of intrusive surveillance techniques such as interception, accessing devices, biometric surveillance, and bulk data analysis must be based on separate judicial orders. Emergency powers should be very specific, specific in time, documented and subject to a subsequent review.

Policies of strong data minimization, purpose limitation and security safeguards should also be implemented in Pakistan. The purpose of the surveillance system should be designated, the time frame should be defined, and the types of data collected should be indicated. There is a need for more protection of sensitive communications between lawyers, journalists, doctors, parliamentarians and religious advisors. Data shall be safely stored, accessed by only authorized people and should be deleted as soon as it is no longer needed.

The personal data protection law must be introduced, and a single Surveillance and Investigative Powers Act may need to be passed in Parliament. These laws must set forth reasonable processing protocols, separate monitoring, judicial review and authorization procedures, transparency and meaningful remedies. The exceptions for national security shall be limited and proportionate, and shall be subject to review, instead of being unlimited.

The existing surveillance systems such as LIMS and web-monitoring platforms need to be legally and technically audited independently to ensure the level of authorisation, access, retention, cyber security risks and compatibility with constitutional rights.

Pakistan needs to establish an independent Surveillance and Data Protection Commission, which will conduct inspections and audits, handle complaints and investigations and publish reports. Transparency reports, parliamentary review and judicial remedies should be commonplace elements of the surveillance regime.

Last but not least, there is a need for special safeguards for biometric and artificial intelligence-based surveillance. Automated systems should not make arrests, investigations or restrictions on individuals without human oversight and legal responsibility (Lognoul, 2025; Wachter et al., 2017). A proper surveillance system should not only protect against abuse, but it should also be effective, necessary and of public benefit, and respect privacy, freedom of expression and democracy.

Conclusion

Digital surveillance can be a proper, legitimate and necessary tool for fighting terror and serious crime, espionage and cyber threats. It can also be a tool of state power that reveals private lives, constructs links and influences language and undermines democratic structures. The Pakistan constitution does not mandate that helplessness on the part of the government is the only choice if one has to do with unconstitutional monitoring. The rights-protective approach to a security order is based on Articles 4, 8, 9, 10A, 14, 19 and 19A, which are the categories that warrant lawful surveillance: categories which are precisely authorized, independently approved, necessary, proportional, audited, and subject to remedies.

The Pakistani record of the recent past shows that there is a need for reform now. The Justice Qazi Faez Isa rulings are related to the dignity, autonomy and independence of institutions and privacy. The 2024 proceedings in the Islamabad High Court (LIMS) show how dangerous it can be for network capability to function outside of a definite authorization chain. These are indicative of wider issues of hidden surveillance, censorship technology and chilling effects that Amnesty International has found in its [2025](#) investigation and rights reports. Meanwhile, the Digital Nation Pakistan Act and developing national architecture of data will bring more and better public sector data.

Comparative experience provides practical advice. Constitutional recognition and proportionality are seen in India, but at the same time, so are the dangers of giving wide exemptions to the state. The detail of the powers, judicial approval, specific supervision and end-to-end safeguards provided by the United Kingdom and the ECtHR demonstrate the importance of these features. EU law applies to retention of data in general, and shows that there are strict limits. The United States and Canada demonstrate the value of provider-held metadata, location records, IP addresses and aggregated observation, which may continue to be private. All these lessons should be merged in a single surveillance law, a thorough and all-encompassing data-protection legislation, an independent commission, a special authorization process, a technical audit regime, transparency and an effective tribunal system in Pakistan.

When power is clearly legal, it is actually made stronger with regard to security. A constitutionally disciplined system focuses limited resources on legitimate threats, adds evidence to the mix, safeguards critical institutions, prevents misuse and holds the public accountable. In the digital age, the most important issue is not whether the state has developed surveillance technology but whether the Constitution applies to each and every part of the technology.

References

- Amnesty International. (2025). Pakistan: Shadows of control: Censorship and mass surveillance in Pakistan - Amnesty International. In *Amnesty International*.
<https://www.amnesty.org/en/documents/asa33/0206/2025/en/>
- Bhatia, G. (2019). *The transformative Constitution: A radical biography in nine acts*. HarperCollins India.
<https://cir.nii.ac.jp/crid/1971993809788603840>
- Big Brother Watch and Others v. United Kingdom [GC], Apps. Nos. 58170/13, 62322/14, and 24960/15 (European Court of Human Rights 2021).
- Binns, R. (2018, January). Fairness in machine learning: Lessons from political philosophy. In *Conference on fairness, accountability and transparency* (pp. 149-159). PMLR. <https://proceedings.mlr.press/v81/binns18a.html>
- Brayne, S. (2021). *Predict and surveil: Data, discretion, and the future of policing*. Oxford University Press.
- Butt, M. F., Saleem, H. A. R., Hashmi, M. A. I., & Bano, N. (2024). The Right to Privacy in the Age of Surveillance: Legal Protections In Pakistan. *ASSAJ*, 2(4), 1449-1458.
<https://assajournal.com/index.php/36/article/view/601>
- Carpenter v. United States, 585 U.S. 296 (2018).
- Centrum för Rättvisa v. Sweden [GC], App. No. 35252/08 (European Court of Human Rights 2021).
- Chambers and Partners. (2026). *Data protection & privacy 2026 - Pakistan | global practice guides | chambers and partners*. Chambers.Com. <https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2026/pakistan>
- Citron, D. K. (2022). *The fight for privacy: Protecting dignity, identity and love in the digital age*. Random House.
- Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism* (Vol. 10). New York: Oxford University Press. https://cyber.harvard.edu/sites/default/files/2019-12/2019_11_21_Berkman_Julie_Cohen_NS.pdf
- Commissioner of An Garda Síochána and Others, Case C-140/20, ECLI:EU:C:2022:258 (Court of Justice of the European Union 2022).
- Council of Europe. (2018). Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223).
- Daudpota, F. (2023). *Pakistan: Overview of its draft data protection act, 2023*. <https://doi.org/10.2139/ssrn.4667042>
- Deibert, R. J. (2020). *Reset: Reclaiming the internet for civil society*. House of Anansi.
- Digital Nation Pakistan Act, No. I of 2025 (Pakistan).
- Digital Personal Data Protection Act, No. 22 of 2023 (India).
- Digital Personal Data Protection Rules. (2025) (India).
- Digital Rights Foundation. (2025). *Digital Security Helpline annual report 2024*. <https://digitalrightsfoundation.pk/>
- DLA Piper. (2026). Data protection laws of the world: Pakistan. <https://www.dlapiperdataprotection.com/>
- EU, G. (2016a). General data protection regulation. *Official Journal of the European Union*.
- European Court of Human Rights, & European Union Agency for Fundamental Rights. (2025). Mass surveillance: Joint factsheet.
- European Data Protection Board. (2021). Guidelines 10/2020 on restrictions under Article 23 GDPR (Version 2.1).
- European Parliament & Council of the European Union. (2016b). Directive (EU) 2016/680 on data processing by competent authorities for law-enforcement purposes. *Official Journal of the European Union*, L 119, 89–131.
- European Union Agency for Fundamental Rights. (2017). Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU—Volume II.

- Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. In *The rise of big data policing*. New York University Press. <https://doi.org/10.18574/nyu/9781479854608.001.0001>
- Freedom House. (2025). Freedom on the Net 2025: Pakistan. <https://freedomhouse.org/country/pakistan/freedom-net/2025>
- Gellert, R. (2020). *The risk-based approach to data protection*. Oxford University Press.
- Greenleaf, G. (2021). *Asian data privacy laws: Trade and human rights perspectives (2nd ed.)*. Oxford University Press.
- Haq, A. H. U. (2024). The right to privacy & personal data protection: An analysis of Pakistan's proposed personal data protection bill. *UCP Journal of Law & Legal Education*, 2(2), 01-27. <https://ojs.ucp.edu.pk/index.php/ucpjle/article/view/122>
- Hildebrandt, M. (2020). *Law for computer scientists and other folk*. Oxford University Press.
- Human Rights Commission of Pakistan. (2025). *State of human rights in 2024*.
- Human Rights Council. (2021). *The right to privacy in the digital age (A/HRC/RES/48/4)*. United Nations.
- Human Rights Watch. (2025, February 3). *Pakistan: Repeal amendment to draconian cyber law*. <https://www.hrw.org/news/2025/02/03/pakistan-repeal-amendment-draconian-cyber-law>
- Human Rights Watch. (2026). *World report 2026: Pakistan*. <https://www.hrw.org/world-report/2026/country-chapters/pakistan>
- Hussain, Z., Chen, M., Yunjiao, X., Abbas, S., & Tabassam, A. (2026). Carbon neutrality through legislation, judicial oversight, and environmental policies in developing countries. *Environment, Development and Sustainability*, 1-34. <https://doi.org/10.1007/s10668-026-07959-1>
- International Bar Association. (2025). The concept of authorisation under Pakistan's data protection bill. <https://www.ibanet.org/>
- International Comparative Legal Guides. (2026). *Data protection laws and regulations: Pakistan 2026*. <https://iclg.com/practice-areas/data-protection-laws-and-regulations/pakistan/>
- Investigatory Powers (Amendment) Act 2024, c. 9 (United Kingdom).
- Investigatory Powers Act 2016, c. 25 (United Kingdom).
- Investigatory Powers Commissioner's Office. (2025). Annual report 2024. <https://www.ipco.org.uk/publication/annual-report-2024/>
- Islamabad High Court. (2024, June 25). Order in W.P. No. 2758/2023.
- Justice K.S. Puttaswamy (Retd.) (Aadhaar) v. Union of India, (2019) 1 S.C.C. 1 (India) (judgment delivered 2018).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
- Justice Qazi Faez Isa v. President of Pakistan, P.L.D. 2021 S.C. 1 (Pakistan).
- Justice Qazi Faez Isa v. President of Pakistan, P.L.D. 2022 S.C. 119 (Pakistan).
- Kaye, D. (2019). *Speech police: The global struggle to govern the internet*. Columbia Global Reports.
- Kerr, O. S. (2018). Implementing Carpenter. *Harvard Law Review*, 132, 617-646. <https://www.lawfaremedia.org/article/implementing-carpenter>
- Khera, R. (Ed.). (2019). *Dissent on Aadhaar: Big data meets Big Brother*. Orient BlackSwan.
- Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.
- La Quadrature du Net and Others, Joined Cases C-511/18, C-512/18, and C-520/18, ECLI:EU:C:2020:791 (Court of Justice of the European Union 2020).
- Leaders of a Beautiful Struggle v. Baltimore Police Department, 2 F.4th 330 (4th Cir. 2021) (en banc).

- Lognoul, M. (2025). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act–AI Act). *Revue du Droit des Technologies de l'information*, (3-4), 145-189. <https://researchportal.unamur.be/en/publications/regulation-eu-20241689-laying-down-harmonised-rules-on-artificial/>
- Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.
- Manohar Lal Sharma v. Union of India, W.P. (Crim.) No. 314 of 2021 (Supreme Court of India, Oct. 27, 2021).
- Mantelero, A. (2022). *Beyond data: Human rights, ethical and social impact assessment in AI*. Springer.
- Ministry of Electronics and Information Technology. (2026). *Establishment of the Data Protection Board of India*. Government of India.
- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. <https://doi.org/10.1177/2053951716679679>
- Munir, A. (2025). Cybercrime laws and digital privacy in Pakistan. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5950694
- Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018).
- National Assembly of Pakistan. (2025). The Constitution of the Islamic Republic of Pakistan (current official edition).
- Office of the United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age (A/HRC/39/29)*. United Nations. <https://www.ohchr.org/en/documents/thematic-reports/ahrc3929-right-privacy-digital-age-report-united-nations-high>
- Office of the United Nations High Commissioner for Human Rights. (2021). *The right to privacy in the digital age (A/HRC/48/31)*. United Nations. <https://www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high>
- Office of the United Nations High Commissioner for Human Rights. (2025). *The right to privacy in the digital age (A/HRC/60/45)*. United Nations. <https://www.ohchr.org/en/documents/thematic-reports/ahrc6045-right-privacy-digital-age-report-office-united-nations-high>
- Organisation for Economic Co-operation and Development. (2022). Declaration on government access to personal data held by private sector entities. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>
- Pakistan Code. (2026a). Pakistan Telecommunication (Re-organization) Act, 1996 (official consolidated text consulted in 2026). Ministry of Law and Justice, Government of Pakistan.
- Pakistan Code. (2026b). Prevention of Electronic Crimes Act, 2016 (official consolidated text consulted in 2026). Ministry of Law and Justice, Government of Pakistan.
- Pakistan Digital Authority. (2026). *Digital governance, data, and AI regulatory framework*. <https://pda.gov.pk/>
- Personal Data Protection Bill. (2023) (Pakistan) (draft).
- Prevention of Electronic Crimes (Amendment) Act, No. II of 2025 (Pakistan).
- Prevention of Electronic Crimes Act, No. XL of 2016 (Pakistan).
- Privacy and Civil Liberties Oversight Board. (2023). Report on the surveillance program operated pursuant to Section 702 of the Foreign Intelligence Surveillance Act.
- Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Case C-623/17, ECLI:EU:C:2020:790 (Court of Justice of the European Union 2020).
- Privacy International. (2017). *The right to privacy in the Islamic Republic of Pakistan: UPR 28th session*. Privacy International. <https://privacyinternational.org/advocacy/834/right-privacy-islamic-republic-pakistan-upr-28th-session>
- R. v. Bykovets, 2024 SCC 6 (Canada).

- R. v. Jarvis, 2019 SCC 10 (Canada).
- Rana, A., & Iqbal, A. (2025). Privacy and surveillance: Legal and technical perspectives. *UCP Journal of Law & Legal Education*, 3(2), 01–28. <https://doi.org/10.24312/ucp-jlle.03.02.552>
- Reforming Intelligence and Securing America Act, Pub. L. No. 118-49 (2024) (United States).
- Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and Abstraction in Sociotechnical Systems. *Proceedings of the Conference on Fairness, Accountability, and Transparency - FAT* '19*, 59–68. <https://doi.org/10.1145/3287560.3287598>
- Solove, D. J., & Schwartz, P. M. (2020). *Information privacy law* (7th ed.). Wolters Kluwer.
- SpaceNet AG and Telekom Deutschland GmbH, Joined Cases C-793/19 and C-794/19, ECLI:EU:C:2022:702 (Court of Justice of the European Union 2022).
- Tabassam, A., & Husaain, Z. (2024). Sustainable resource management and economic development: evaluating the impact of rare earth mining on local economies and environmental sustainability in China. *Journal of Environmental Science and Economics*, 3(4), 1-11. <https://doi.org/10.56556/jescae.v3i4.997>
- Tele2 Sverige AB and Watson, Joined Cases C-203/15 and C-698/15, ECLI:EU:C:2016:970 (Court of Justice of the European Union 2016).
- Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.
- United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (en banc).
- United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021).
- Véliz, C. (2020). *Privacy is power: Why and how you should take back control of your data*. Bantam Press.
- Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019(2), 494–620. <https://doi.org/10.31228/osf.io/mu2kf>
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76–99. <https://doi.org/10.1093/idpl/ix005>
- Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. <https://doi.org/10.31228/osf.io/jq2b6>
- Wajahat, J., Tarana, M., & Gul, S. (2025). Vague Laws and Digital Censorship: The Constitutional Challenges of the Prevention of Electronic Crimes Act (PECA) Amendments, 2025. *The Lighthouse Journal of Social Sciences*, 4(01), 1-12.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.