

Unveiling the tapestry: a comparative investigation into data-protection legislation in India and Pakistan

Muhammad Imran Ali*, Khadeeja Ahmad Hussain**

*Lahore Leads University, Pakistan, Imran.ali@leads.edu.pk, ORCID: 0000-0003-1395-229X

***Lahore Leads University, Pakistan, khadeejahussain.law@leads.edu.pk, ORCID: 0009-0008-4274-0695

Abstract

In today's digital interconnectedness, data regulation in South Asia, particularly in India and Pakistan, is transforming into a state where profound changes are occurring. This article deals with the contrastive analysis of personal data-protection laws in the two countries, with the aim of revealing the points of convergence and divergence and the reasons that either support or reject unification. Different approaches led to the development of these standards, which encompass varying levels of scope, complexity and risk. The methodology prescribes reviewing and assessing the existing laws and proposing their legislative development. The research exposes the inefficiency in the legislative aspect of dealing with the rising demand for an adequate regulatory framework for data-protection measures. The wisdom drawn from this examination bestows priceless advice on Politician's, legal experts and all involved parties who are concerned about data protection in the context of digital connections. International best practices can be adapted to inform reforms of the Digital Personal Data Protection (DPDP) Act, 2023, in India and the proposed Personal Data Protection Bill, 2023, in Pakistan to bring enhanced regimes for comprehensive and effective personal data protection in both nations.

Keywords

data-protection laws • India • legislation • Pakistan

INTRODUCTION

Digital privacy is important today due to the simplicity with which personal information is accessed and controlled online. With the increase in our digital footprint, protection of sensitive information from abuse or unauthorised access is critically essential (Aldawood and Skinner, 2019). Despite the tremendous progress of technology, there are questions concerning the morality and legality of data privacy (Quach et al., 2022). The age of the Internet unquestionably not only brings pleasure but also generates concerns regarding privacy and data safety. As our lives become increasingly intertwined with online platforms, this has led to the requirement of robust digital privacy and data-protection laws. Laws that govern the collection, use and disclosure of personal information by organisations, governments and other entities. With the growing importance of data itself, threats of possible maltreatment and improper use of personal information come to light (Wang et al., 2023). Such rights and freedom are being implemented by laws, for instance, GDPR in the European Union, by different governments worldwide (Ducato, 2020). In the United States, the Privacy Act of 1974 regulates the federal government's handling of personally identifiable information (PII). The Children's Online Privacy Protection Act

(COPPA) safeguards children. The Health Insurance Portability and Accountability Act (HIPAA) protects healthcare privacy. The California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) empower consumer data control. In the United Kingdom, the Data Protection Act, 2018, aligns with the GDPR for personal data oversight, promoting global privacy standards.

The South Asian area, which is mainly composed of India and Pakistan, is experiencing a comparable rate of internet penetration and technology adoption. As such, the region needs a robust legislative framework to preserve its inhabitants' digital footprints (Bentotahewa et al., 2022). Such rapid digitalisation forces us to use data-driven processes, which need to defend the privacy of the human being (Islam et al., 2022). India has got data-protection laws in full measure, with the Digital Personal Data Protection Act, 2023, coming as a good example that looks at user consent and accountability. The Personal Data Protection Bill, 2023, was also introduced in the parliament of Pakistan, with an emphasis on data collection, processing and storage. Unfortunately, this bill is still awaiting authorisation. What both countries have to deal with is how to combine technological progress with the individual's right to privacy, and their further improvement of these legal frameworks is a key issue in the establishment of a safe online environment (Gregory, 2024). Policymakers in Pakistan and India should introduce relevant

*Corresponding author:

preventive measures to counter the increasing risks that will undermine the efficiency of their digital privacy and data-protection laws. This article analyses the complexity of data-protection legislation in India and Pakistan in the context of technological advancement and, in particular, how these legislation frameworks work. It is an important policy instrument for stakeholders, legal practitioners and policymakers, with a socio-legal-oriented perspective on reform in data protection.

RESEARCH RESULTS AND DISCUSSION

An overview of digital privacy and data-protection laws

The modern era is characterised by the extensive use of digital technology and connected devices, which has led to issues related to digital privacy. To protect the privacy of every individual, governments and regulatory authorities all over the globe have put in place data-protection policies (Tawalbeh et al., 2020). In 2018, the European Union came up with the General Data Protection Regulation (Regulation EU, 2016) to give individuals the right to control their personal data and also to ensure that companies practice morality in using it (Yuan and Li, 2019). Transparency, consent and purpose limitation are the main principles of the GDPR, which imply the need for companies to share how they collect, process and store private data. Users must provide consent in a clear manner that their data will be processed, and the purposes for which their information will be used should be detailed. Due to this change in data management, there are ethical and user-centred practices. Outside of the European Union, several countries have modernised their data-protection laws to cater to the dynamic digital environment, such as the CCPA (2016) in the United States. Nevertheless, the siloed nature of the laws across state borders creates problems for businesses that operate across state borders; so, an ideal solution would be a federal privacy framework.

Positive effects of the digital privacy regulations exist, although there are still some challenges, especially as to how to maintain balance between privacy and the monetisation of personal data (Schäfer et al., 2023). Most of the platforms are based on targeted advertising, for which user data collection and analysis are required. The task of balancing business interests against individual privacy rights is a sensitive one, and it necessitates permanent dialogue and cooperation among all the stakeholders, including policymakers, industry representatives and privacy activists. The global character of the internet poses issues concerning the extraterritorial application of data-protection laws, rendering their enforcement difficult. Ensuring uniform global standards and promoting collaboration among countries become necessary

to build a compact global system for the privacy of digital information (Çapar, 2022). The digital era has created major privacy challenges; however, data-protection laws such as The Privacy Act (The Privacy Act, 1974) regulate the functionalities of the federal government in the management of PII in the United States. It gives individuals a right to records held by federal agencies, and it saves PII disclosures without consent. The COPPA (Children's Online Privacy Protection Act, 1998) is a framework for online privacy protection for children. It demands proof of parental consent before collecting private information from children under Section 13. The Health Insurance Portability and Accountability Act (HIPAA, 1996), which protects health information and prohibits violations of the privacy of the person in the healthcare setting, was enacted in 1996. In 2018, the CCPA (The California Consumer Privacy Act, 2018) empowered local consumers to control the data collected by companies, resulting in clearer procedures and more protective measures. The California Privacy Rights Act (CPRA, 2020), effective January 2022, is a better version of the CCPA in many respects. It shows high privacy standards; it is about new rights and the establishment of a dedicated enforcement agency. The British Data Protection Act (The Data Protection Act, 2018) reconciles with the GDPR, which is used to monitor personal data processing and is assured by the ICO; hence, accountability and transparency are observed. With the advancement of technology, privacy regulations need to change to deal with new challenges more efficiently (Kumar et al., 2019). Protection of digital privacy is not only a legal and regulatory issue but also a societal effort to harmonise technological progress with basic human rights in the digital age (Smitha and Sharngan, 2021).

Data-protection laws in India

Major changes in the Indian data-protection laws are taking place with the introduction of the Personal Data Protection Bill (2019) and the Digital Personal Data Protection Bill (2022) in relation to cross-border data flows, surveillance, and individual rights. The Digital Personal Data Protection Act (2023) sets up a strong legal regime for processing personal data and strengthens concepts of consent, data minimisation and purpose limitation. Thus, legislative moves prove that India is ready to improve its legal framework according to rapid digital development and is paying attention to promoting individuals and responsible data practices of companies in the country. The objective is to make individuals more powerful and promote the responsible use of data by entities operating within the nation.

Personal Data Protection Bill 2019, India

The draft Personal Data Protection Bill (2019) was crafted by the B.N. Srikrishna Committee, echoing the report 'A Free and Fair Digital Economy: The Report Protecting Privacy,

Empowering Indians'. Advocating a global legal framework for safeguarding PII, the Committee highlights the importance of data subject permission (Committee of Experts, 2018). The bill establishes the Data Protection Authority (DPA) of India, signifying India's legislative recognition of the right to erasure. The Personal Data Protection Bill, 2019, in India mandates data fiduciaries to obtain consent, limits data-processing purposes, emphasises necessity in data collection, ensures transparency through notice and enforces standards for data quality, retention and accountability. Chapter III delineates grounds for processing data without consent, with Section 13 for employment-related cases and Section 14 for reasonable purposes. Section 15 categorises information as sensitive, addressing increased concerns about privacy. The legislation also emphasises the protection of children's data and provides comprehensive rights for individuals regarding their data, including confirmation, access, correction, deletion, data transferability and the right to be forgotten. Chapters VI–XIII of the bill delve into aspects of data protection such as transparency, accountability, limitations on data movement, exemptions, the establishment of a DPA, penalties for non-compliance with regulations and the prevention of data-related offenses. They encompass privacy policies, breach notifications, enforcement actions and coordination efforts to ensure adherence to rules governing data management.

This bill, however, establishes a framework with several deficiencies. Section 4 may encounter challenges in obtaining user consent due to terms and conditions, while Section 6 might permit data collection based on vague justifications. Chapter III, Section 12, treats unauthorised processing relating to the problem of abuse. Section 15 is focused on the classification of sensitive data; however, more precise definitions and guidelines are required to eliminate subjectivity. Section 16 is concerned with the protection of children's data; nonetheless, matters such as age verification have to be addressed. Chapter V grants rights to strong data subject to such a character, but their effect is a function of practicability and awareness. Penalties and compensation in Chapter X will, however, discourage small businesses and creativity, while Section XIII increases the uncertainties mostly in re-identification, making enforcement not very possible. The bill's progress depends on implementation, awareness programs and continuous adjustment to address various issues in the growing sector of personal data protection (PDP).

Digital Personal Data Protection Bill, 2022, India

In August 2022, the Indian Ministry of Electronics and Information Technology pulled back the Personal Data Protection Bill, 2019, due to public inputs. On 18 November 2022, the revised bill became public. This act is supplementary to the existing legislation, such as the IT rules, the National Data Governance Framework Policy and the new Digital

India Act. The Indian Digital Personal Data Protection Bill, 2022, aims to safeguard the rights of the individual and the principles of lawful data processing, which creates liability on the part of data fiduciaries. They are bound to pay penalties if they breach any of the provisions stipulated by this law. It fosters the growth of the digital economy via principles like consent and governance that respect the rights of people to access and correct their information. It is the duty of data owners to prevent security issues and breach notification, with parents having to provide consent for their children's data. Such exemptions would cover security services and research. Breaches will be handled by the Data Protection Board through fines and possibly prison sentences (upon subsequent offences), guaranteeing stable digital data protection necessary for secure digital innovation.

Such a balancing bill can be assessed with a particular lack of detail in terms of the obligations of data fiduciaries. There are worries over compliance by NGOs, fines' effectiveness and agencies involved in intelligence activities as an exception. The bill neglected typical modern issues, for example, algorithmic tracking and claim curation. We may need to make some adjustments to the entire opt-in data-protection system, considering both its progressive and imperfect elements, which necessitates careful reflection.

Digital Personal Data Protection Act, 2023, India

In August 2023, the Indian Parliament passed the Digital Personal Data Protection (DPDP) Act, marking the country's first comprehensive law on PDP. Enacted after 5 years of deliberations, this Act was the second version of the bill that was introduced in the Parliament. The Act was preceded by a land-mark judgement in Justice K.S. Puttaswamy's case (Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors., 2017), which recognised privacy as a part of the right to life. The DPDP Act (Digital Personal Data Protection Act, 2023) eases the data-processing laws pertaining to Indian citizens and Indian business houses but gives the central government the option to have discretionary power at times. It is also relevant to non-citizens whose processing is conformed to the delivery of goods or services to those outside the border, whereby the non-citizen has directly offered the services. Personal data may be processed in the interests of lawful purposes where there is free, specific, informed, unconditional and unambiguous consent. Data should be restricted to the intended use, and consumers should be made aware of their rights and grievance-redress mechanisms. Revocation of consent is possible if it serves as the foundation for data processing (Sundara and Narendran, 2023). The DPDP Act therefore endorses legitimate uses that include voluntary provision, consent to state services, security concerns, legal obligations and compliance with judgements. However, granting government agencies the permission

to access stored data may result in privacy and security concerns.

The DPDP Act gives an individual the right to information about data, sharing data and correcting or erasing his or her data. Security should be guaranteed by data fiduciaries, and breaches should be reported to the Data Protection Board of India. Deletion is necessary following the withdrawal of consent or after a determined objective. The act requires a data-protection officer, grievance-redress mechanisms and parental consent for minors. The DPDP Act modifies the regulatory structure in India by replacing the DPA with a new framework. This affects the oversight and enforcement mechanisms, moving away from the Data Protection Bill 2019 model of an independent regulatory authority acting like the EU (GDPR) enforcing agencies. The DPDP Act in India introduces the first Indian data-privacy law that mandates consent for the processing of personal data, gives consumers the right to access, correct, update, and erase their data and provides safeguards for the processing of children's data. Businesses have limitations, duties and safety barricades. The Data Protection Board monitors complaint-resolution mechanisms.

On the other hand, the DPDP Act (Digital Personal Data Protection Act, 2023) has some drawbacks, such as enabling the government to bypass consent requirements for state benefits, exempting government agencies from purpose limitations and providing wide exemptions for some state agencies. None of the approved provisions of Section 17(1)(c) contain any specific operational details, but the government may declare non-application of some provisions of the law to businesses or classes for a period of 5 years. Start-ups are already given some exemptions under Section 17(3), and the open-ended nature of Section 17(5) is problematic. Section 9(1) to Section 9(3) requires, among others, parental consent and profiling prohibition, while Section 9(4) allows the government's exemption from business but does not give clarity on the grounds, conditions and assessment criteria. The composition of the Data Protection Board is also unsuitable in that the government dictates membership with no specification as to the size of the board, and only one legal expert is mandated. Delegating the chairperson powers to consent that any member undertakes vital roles is devoid of an internal separation, thus posing impartiality. Ambiguities in the DPDP Act can spoil its purpose if not implemented carefully. The law depends on the scrupulous fulfilment of its provisions by the government.

Data-protection laws in Pakistan

In today's information-driven world, electronic transactions are gaining popularity, thereby requiring the confidentiality and privacy of personal data. The absence of specific data-protection laws in Pakistan has resulted in the need for a

privacy policy; however, legal responsibilities, contemporary needs and international practices have enforced the development of a privacy policy (Bentotahewa et al., 2022). In Pakistan, three data-protection bills, namely, the Personal Data Protection Bill, 2018, the Personal Data Protection Bill, 2021 and the Personal Data Protection Bill, 2023, have been introduced in parliament up until now.

Personal Data Protection Bill, 2018, Pakistan

The Personal Data Protection Bill, 2018, outlines the details associated with personal data processing under Sections 4–10; these sections exist to aid data controller obligations. The last part of the chapter explains the PDP rights too, including access, rectification and consent withdrawal. The aim of Chapter IV is to explain sensitive data processing. This section (Chapter VI) introduces NCPDP, which is the National Commission for Personal Data Protection. Chapter VII focuses on complaint procedures and crimes such as substantial compounding and corporate liabilities. The said bill intends to guarantee strong data procedures, confidentiality and security with enforcement and redressal mechanisms, thus showing that the country deploys all means to protect individual privacy and create trust in data-management practices.

The Personal Data Protection Bill, 2018, under Chapter II, lays out personal data processing and data controller obligations. Section 4 is unclear in defining 'protection', so it causes confusion. Section 5 covers fundamental rules that may hinder its implementation. Section 6 is defective in giving the procedures for notifying the data subject. Section 9 tries to ensure security and confidentiality, but the attempt seems inadequate. Enforcement is characterised by the absence of severe penalties for the violation of rules. Such divergences highlight the significance of a precisely designed platform for different implementation and compliance areas so that the bill will work efficiently.

Personal Data Protection Bill, 2021, Pakistan

The Personal Data Protection Bill (Personal Data Protection Bill, 2021) was an important move towards the creation of a complete system for Pakistan's PDP, seeking to be an answer to the digital apprehension of data security and privacy, its main component including a definition of the rights of the people to their data. The bill was a new regulatory mechanism for the digital use and management of personal data. However, the bill's various sections provide a comprehensive set of provisions aimed at protecting individual privacy, while also setting excellent standards for the use of personal data. The bill had given more attention to safeguarding the privacy of citizens not only in domestic data processing but also in cross-border situations (Muhammad et al., 2022).

The Personal Data Protection Bill, 2021, is a legislative

framework designed to protect people's rights and privacy in a digitised society. It defines 'data subject' and 'personal data', with data subjects being natural persons who are the object of treatment for personal data. The bill defines three terms: 'data controller', 'data processor', and 'processing'. Data controllers can obtain personal data, while data processors perform data-processing activities. The bill provides more rights to data subjects, including the right to deletion, access, rectification and withdrawal of consent and prohibits harmful processing. Data controllers are required to ensure consent, that processing does not exceed limits and that there is a legitimate purpose for processing data. A commission that has been proposed to be created to secure personal data, protect data subjects' rights, prevent misuse, educate and address complaints. Penalising provisions include imprisonment and fines.

The bill aimed at building rights and protecting personal data in the digital world of Pakistan. Yet, one of the main problems is the unlimited power that data controllers can get if they happen to abuse the given power and tend to centralise it. The main issues surrounding the bill are to get authority for data processing, particularly obtaining informed consent. Heavy penalties and fines can mute the use of the internet, and small businesses may find it hard to bear, whereas big companies would not feel the negative impact. A National Commission was proposed to establish it, which is notable but raises several questions about its functionality in the digital environment, which is changing rapidly. If enacted, this bill is likely to deal with some crucial data-privacy issues, but its broad definitions of data, lack of an opt-in consent system and reliance on punishment can be challenged in order to have a fair and effective system.

Personal Data Protection Bill, 2023, Pakistan

The objective of the Personal Data Protection Bill (Personal Data Protection Bill, 2023) is to provide adequate frameworks for secure data processing. Section 3 specifies the function, authority and range of PDP. The beginning and ending of the coverage are also mentioned. Section 6 of the Act specifies the situations under which personal data handling is possible or not. It should be noted that a declaration of consent is initiated as a fundamental requirement.

The bill requires tight security measures as in Sections 9–12, the data-preservation guidelines and the rules for the security of data integrity in these sections. In the context of children, Section 14 deals with the processing of personal data. Sections 16–29 specify the rights of data subjects like access, rectification, withdrawal of consent, objection to distressing processing, erasure, nomination, complaint and portability. Sections 30–32 limit data transfer, providing conditions and structures for cross-border data transfer. Sections 35–39 create the Commission as the regulatory authority, defining its

structure, functions and powers. The Commission is charged with monitoring data-protection actions. Sections 48–50 give the Commission the power to impose enforcement orders, fines for wrongful processing and failure to undertake any security measures. Sections 51–52 offer ways of making a complaint by individuals, and appeals against decisions of the Commission are provided for. Sections 53–55 contain the interim provisions and empower the authority to lay down the rules and regulations to ensure proper functioning. Section 56 is dedicated to the relationship between the Act and other statutes, while Section 58 addresses the procedure concerning the liquidation of the regulatory authority. Basically, the Personal Data Protection Bill, 2023, deals with bodies like consent, security, individual rights, cross-border data transfer, regulatory oversight and enforcement mechanisms. It seeks to achieve a middle ground between the privacy of personal data and its useful access, which is a trend in a number of countries to have strong data-protection regulations.

The Personal Data Protection Bill, 2023, appears to address many important aspects of data protection, but some significant shortcomings deserve attention. Section 6 is specific for the need for explicit consent and is silent on how to handle situations when consent is not possible, which might lead to a lack of clarity. Sections 9–12 about security and retention may impose an unnecessary burden on businesses with few benefits, needing flexible provisions suitable for different industries. Section 14 is good about how it talks about children's data, but without ages and how to verify consent, it will put children's privacy at risk. Although Sections 16–29 outline data subjects' rights exhaustively, the bill is silent on the implementation of such rights and their enforcement, limiting protection. The chapters 30–32 based on cross-border data transfer need strong mechanisms that should clearly specify criteria for evaluating the data-protection adequacy of recipient countries. The Commission, as stated in Sections 35–39, is a positive development, but the lack of independent provisions is worrying. Clear-cut rules on Commission member selection and elimination could improve credibility. Sections 48–50 provide enforcement powers, but there is no proportional approach to sanctions in the bill, implying a more balanced attitude that promotes compliance without stifling innovation. In summary, although the Personal Data Protection Bill, 2023 resonates with the world trend, rectifying the noted deficiencies is key to a comprehensive and efficient platform for the protection of personal data in Pakistan.

A comparative analysis of data-protection laws in India and Pakistan

The introduction of the DPDP Act, 2023, in India and the Personal Data Protection Bill, 2023, in Pakistan are the first steps towards data protection. The Indian DPDP Act can

realistically meet parameters. It bestows the authority to simplify procedures on the government while granting it very wide powers. This may also invite doubts about uncontrolled authority. The Act includes residents of the United States, American companies, and non-citizens who are related to the import of foreign goods or services. Still, the DPDP Act, which places emphasis on the necessity of prior consent for data profiling and utilisation, is backed by the fact that personal data processing for legitimate purposes is allowed (Kuner, 2021). Nevertheless, such a scenario raises questions about government agencies being able to have access to information stored by other entities, which can be a threat to data safety and privacy. The DPDP Act institutes strong individual rights, including the right to access, modify and erase personal information. The data fiduciaries need to guarantee the security and accuracy of the data and report data breaches to the DPB. The Act prescribes for data-protection officers, grievance-redress mechanisms and specific provisions for minors. Conversely, government exemptions lack clear guidelines, but they create a hindrance to the effectiveness of child-protection measures. What is particularly interesting is that the DPDP Act fails to follow the initially outlined regulation model and substitutes the planned Indian DPA with a new regulatory structure. This transformation of the systems of supervision and control is a departure from the earlier scheme that was compared with EU data-protection agencies. The Act is the first data-privacy law in India and requires prior consent for the processing of personal data with limited exceptions, giving consumers robust rights and businesses definite obligations.

India boasts a wealth of global privacy legislation that guides the establishment of a comprehensive data-protection framework. The Privacy Act of 1974 brought transparency and accountability at the federal level through the data gathering of government agencies in the United States, which has proved useful as a procedural model. The Children's Online Privacy Protection Act, 1998 (COPPA) attaches gloves to a minor's protection over the internet with an accent at the concurrence of parental consent and data minimisation. Besides, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 also establishes the need to keep sensitive health information safe and to be strict about its enforcement. At the regional level, we can emulate and use the CCPA (CCPA), 2018 and the California Privacy Rights Act (CPRA), 2020. The UK Data Protection Act was formulated by the UK government with the purpose of providing safeguards to people in cases where their data and its ownership rights are at risk and also creating bodies to oversee breaches of data. As for the new DPDP Act in India, it is hoped that the provision will include some of these aspects, ensuring that personal data is respected, holding data controllers accountable and permitting the mechanisms

to address the grievance. Through integrating different views, India can create an approach that ensures not only effective protection but also protection that is aligned with Indian values and garners trust among all states, promoting peace and prosperity online.

The Personal Data Protection Bill 2023, Pakistan, introduces a robust instrument for the preservation of personal data. It starts with the declaration of lawful consent for processing and also includes stringent security measures, retention rules and data-integrity principles. Furthermore, it touches upon some children's data protection and defines particular requirements for data movement across borders. The bill establishes a commission with enforcement abilities to be set up through this regulation and gives it the power to issue orders, impose fines and deal with complaints and appeals that are made in this regard. On the other side, it ensures compliance and accountability (Javed, 2023). Currently, the Personal Data Protection Bill, 2023, is still under review in the Pakistani Parliament.

The draft Personal Data Protection Bill, 2023, has the potential to reflect those insights and provide Pakistan with an opportunity to enhance its global privacy legislation standards. The USA Privacy Act of 1974 brings transparency and accountability to data processing; thus, it is the main example of country data protection. Similarly, the COPPA brings attention to the need for specialised defences for children, with announced user consent and limited collection of data. HIPAA illustrates the need for thorough legislation that ensures the safety of medical data for patients. The CCPA and CPRA are two state-level legislations that promote consumers' rights, provide substantial remits and have formidable enforcement. The principles of GDPR are followed by the Data Protection Act, UK, which is practical, but sometimes restrictions can occur and therefore can be considered an effective regulatory system. By embracing these perspectives, Pakistan can guarantee that the data-protection bill is at the cutting-edge level of the world's best practices while also protecting the country's national interests, thus creating an atmosphere of trust and technological progress.

CONCLUSION

Both the DPDP Act (DPDP), 2023 in India, and the Personal Data Protection (PDP) Bill, 2023 in Pakistan, are endeavours that aim to deal with problems connected with the usage of personal data on the internet. With the adoption of DPDP in India and the proposed PDP Bill in Pakistan, steps are being taken to guarantee the online privacy of individuals. In India, DPDP lays down the principles related to the collection, storage and processing of data, such as international standards, by private entities. Nevertheless, adherents will

point out the dissemination gaps in information and question the implications of government surveillance. Pakistan's PDP Bill is a long-overdue move to protect an individual's privacy rights from ongoing invasion during rapid technological development. The legislation looks to reprimand private companies for violating norms such as the US, UK, and EU's GDPR. It provides restrictions on data usage, including consent, limitations on purpose and minimisation of information when transparency and accountability are needed.

In contrast to the well-established legislation like the US Privacy Act and the UK Data Protection Act that provide frameworks, these initiatives by India and Pakistan appear to be more fragmented and thus spontaneously developed. Regulations are designed for openness, the user's control and responsibility that are adopted by different industries, making it possible for data-management procedures to be put in place. India and Pakistan can make headway on this issue by updating the enforcement mechanism, integrating data breach alerts and forming independent oversight bodies that will be in charge of monitoring implementation. There is a need to follow new technologies, such as AI and IoT, and implement measures of privacy to avoid potential risks. Presumably, the settlement with the data-transfer frameworks of the standards helps to drive data flow while meeting the privacy standards. The DPDP Act of India and the proposed PDP Bill in Pakistan are two steps forward in privacy and data-protection laws. Although gaps in the existing legislation can be overcome through inclusions and processing deficiencies as guidelines, the effectiveness of thorough privacy laws can be further developed in the digital era to protect the rights of individuals.

REFERENCES

- Aldawood, H., Skinner, G., (2019). Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues. *Future Internet*, 11 (3). 73. <https://doi.org/10.3390/fi11030073>.
- Bentotahewa, V., Hewage, C., Williams, J., (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science*, 3. 183. <https://doi.org/10.1007/s42979-022-01079-z>.
- California Legislature. (2018). The California Consumer Privacy Act (CCPA).
- California Legislature. (2020). The California Privacy Rights Act (CPRA).
- Çapar, G., (2022). Global Regulatory Competition on Digital Rights and Data Protection: A Novel and Contractive form of Eurocentrism? *Global Constitutionalism*, 11 (3). 465–493.
- Committee of Experts. (2018). A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians. Retrieved from: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.
- Digital Personal Data Protection Act. (2023). Retrieved from: <https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>
- Digital Personal Data Protection Bill. (2022). Retrieved from: https://www.meity.gov.in/writereaddata/files/The%20Digital%20Personal%20Data%20Protection%20Bill%20C%202022_0.pdf
- Ducato, R., (2020). Data Protection, Scientific Research, and the Role of Information. *Computer Law & Security Review*, 37. <https://doi.org/10.1016/j.clsr.2020.105412>.
- Greenleaf, G., (2011). Promises and Illusions of Data Protection in Indian Law. *International Data Privacy Law*, 1 (1). 47–69.
- Gregory, P.C., (2024). The Diffusion of Data Privacy Laws in South-east Asia: Learning and the Extraterritorial Reach of the EU's GDPR. *Contemporary Politics*. <https://doi.org/10.1080/13569775.2024.2310220>.
- Islam, M.T., Sahula, M., Karim, M.E., (2022). Understanding GDPR: Its Legal Implications and Relevance to South Asian Privacy Regimes. *UUM Journal of Legal Studies*, 13 (1). 45–76.
- Javed, A.M., (2023). Cyber Security and Data Privacy Laws in Pakistan: Protecting Information and Privacy in the Digital Age. *Pakistan Journal of International Affairs*, 6 (3). 356–366.
- Justice, K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. (2017) AIR SC 4161.
- Kumar, S., Tiwari, P., Zymbler, M., (2019). Internet of Things is a Revolutionary Approach for Future Technology Enhancement: A Review. *Journal of Big Data*, 6 (111). <https://doi.org/10.1186/s40537-019-0268-2>.
- Kuner, C., (2021). The Path to Recognition of Data Protection in India: The Role of the GDPR and International Standards. *National Law School of India Review*, 33 (1). 69–91.
- Muhammad, S.A., Kashif, M.S., Hamid, M., Hafsa, N., (2022). An Analysis of Data Privacy and Protection Laws in Pakistan. *Russian Law Journal*, 10 (4). 142–147.
- Personal Data Protection Bill. (2018). Retrieved from: <https://moitt.gov.pk/SiteImage/Downloads/Personal%20Data%20Protection%20Bill%20without%20track%20changes.pdf>.
- Personal Data Protection Bill. (2019). Retrieved from: http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.
- Personal Data Protection Bill. (2021). Retrieved from: [https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft\(1\).pdf](https://moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft(1).pdf).
- Personal Data Protection Bill. (2023). Retrieved from: <https://moitt.gov.pk/SiteImage/Misc/files/Final%20Draft%20Personal%20Data%20Protection%20Bill%20May%202023.pdf>.
- Quach, S., Thaichon, P., Martin, K.D., Weaven, S., Palmatier, R.W. (2022). Digital Technologies: Tensions in Privacy and Data. *Journal of the Academy of Marketing Science*, 50. 1299–1323.
- Regulation (EU). (2016). General Data Protection Regulation, 679. Retrieved from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

- Schäfer, F., Heiko, G., Christoph, G., Oliver, G., Felix, W., (2023). Data-Driven Business and Data Privacy: Challenges and Measures for Product-Based Companies. *Business Horizons*, 66 (4). 493–504.
- Smitha, K.P., Sharngan, A., (2021). Playing Catch Up-Privacy Regimes in South Asia. *The International Journal of Human Rights*, 25 (1). 79–116.
- Sundara, K., Narendran, N., (2023). The Digital Personal Data Protection Act, 2023: Analysing India's Dynamic Approach to Data Protection. *Computer Law Review International*, 24 (5). 129–141.
- Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, 10 (12). 4102. <https://doi.org/10.3390/app10124102>.
- The California Consumer Privacy Act of 2018. (2018). Retrieved from: https://coppa.ca.gov/regulations/pdf/coppa_act.pdf.
- United Kingdom Parliament. (2018). Data Protection Act 2018, c. 12, UK.
- United States Congress. (1974). The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
- United States Congress. (1996). The Health Insurance Portability and Accountability Act (HIPAA), 1996 Public Law 104-191.
- United States Congress. (1998). Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6505.
- Wang, M., Qin, Y., Liu, J., Li, W., (2023). Identifying Personal Physiological Data Risks to the Internet of Everything: The Case of Facial Data Breach Risks. *Humanities and Social Sciences Communications*, 10. 216. <https://doi.org/10.1057/s41599-023-01673-3>.
- Yuan, B., Li, J., (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Environmental Research and Public Health*, 16 (6). 1070. <https://doi.org/10.3390/ijerph16061070>.