UCP Journal *of* Law & Legal Education
Vol. 2, Issue 2 (January - June 2024)

The Right to Privacy & Personal Data Protection: An Analysis of Pakistan's Proposed Personal Data Protection Bill

Aly Hassam Ul Haq*

Abstract

The fundamental idea of personal data protection is to ensure that individuals (formally known as 'data subjects') have control over the collection, use and inferences made from their personal data. It is, therefore, imperative to grant effective knowledge and control to the data subject since [digital] data collection is prevalent in virtually every e-service or digital platform. As a result, user data has become more vulnerable than ever. To overcome exposure issues created by personal data breaches, various jurisdictions have implemented laws that provide for the rules with which personal data is to be collected, processed and disseminated. Following suit, the Government of Pakistan has taken the initiative to protect the privacy and personal data of every citizen through the [prospective] promulgation of the Personal Data Protection Bill, 2021. This is no doubt a pertinent step towards a better and digitally-secure future for Pakistan. However, although the Bill purports to be a sui generis solution to all matters pertaining to personal data protection, it appears to be ineffective in upholding the fundamental principles which are derived from international best practices. This paper studies the philosophical basis for the right to privacy to be expanded to cover the requirements of the digital age, aligned with the use-case scenarios which have emerged after the concept of the right to privacy was initially posited. The Bill is then juxtaposed against international best-practices and analysed as to the efficacy of the implementation of the principles of personal data protection. In conclusion, recommendations for amending the Bill are posited.

Keywords: Data Protection, Personal Data Protection, The Right to Privacy, Digital Technology, Surveillance

***Director, Centre for Law & Technology, Faculty of Law, Politics & Governance, Ziauddin University, Karachi, Pakistan. email: aly.hassam@zu.edu .pk
Article History: Received; 20 June 2023; Received in revised form 01 January 2024; Accepted: 05 March 2024
Available online: 15 August 2024

Introduction

> *"Personal data is the new oil of the internet and the new currency of the digital world"* (Kuneva, 2009).

Personal data is one of the most prolific commodities in the digital economy. Not only can the holder of swathes of personal data make meaningful inferences about people, but can also use data points to create a psychological profile on data subjects, without their explicit knowledge in some cases. Particularly where personal data protection legislation exists at a comparable level to the European Union's General Data Protection Regulation, 2018, data subjects are afforded protection against automated decision-making as well as profiling.

The fundamental idea of personal data protection is to ensure that individuals (formally known as 'data subjects') have control over the collection, use and inferences made from their personal and sensitive data. It is, therefore, imperative to grant *effective* knowledge and control to the data subject since [digital] data collection is prevalent in virtually every e-service or digital platform.[1] As a result, user data has become more vulnerable than ever. To overcome exposure issues created by breaches of personal data, various jurisdictions have implemented laws which provide for the *rules* with which personal data is to be collected, processed and disseminated. Following suit, the Government of Pakistan has taken the initiative to protect the privacy and personal data of every citizen through the [prospective] promulgation of the Personal Data Protection Bill, 2021. This is no doubt a pertinent step towards a better and digitally-secure future for Pakistan (The Correspondent, 2021).

A strong and transparent data protection law is the need of the hour, economically. With the incumbent government focusing on foreign remittances, having a balanced law with respect to data protection may encourage international concerns to set up- or rely on- Pakistan-based data centres. Such a paradigm will put Pakistan in a much more favourable position as compared to its southeast Asian neighbours. The Personal Data Protection Bill of 2021 (the

[1] 'Platform' in this context also refers to digital hardware which is capable of collecting and/or making inferences from data, i.e. smart phones, laptops, tablets, etc.

'Bill')- if amended- would be a much-needed addition to the legislative landscape for the protection of personal data- which is linked to the 'right to privacy' (as enshrined in Article 14 of the Constitution). The Bill has been received with a mix of scepticism and appreciation by civil society and commercial stakeholders alike. Where most expectations were met with regard to protecting personal data, the exceptions thereto dilute the efficacy of what the Bill originally purported to offer in its first draft of 2018.

We have seen Pakistan struggle to stay up to speed on legislative affairs- regardless of which political party is leading the House. Perhaps the most recent example is the promulgation of the Geographical Indication (Registration and Protection) Act, 2020. Experts had long been advocating for the necessity of recognizing geographical indicators in Pakistan, however, the European Union-based Basmati rice case *versus* India was the final push needed to spring the legislative machinery into action. It can only be hoped that a similar push is not needed for the Parliament to pass adequate data protection legislation. The WhatsApp privacy policy quandary has been a similar push, however, to date, there are no amendments to the Bill (following the quandary) which reflect that the law would be effective. Although the Bill aims to consolidate positives in terms of commercial feasibility, ease of access for law enforcement and respecting individual rights, it invariably leans towards the first two at the expense of the individual. Such a position may be argued to be fair, given the socio-political and cultural context of Pakistan, however, if the state is to remain relevant in the international arena, the Bill must be heavily modified. [2]

It is now time to work towards an effective legislative regime pertaining to personal data protection in Pakistan. Some may argue that the ship has already sailed. However, as the saying goes- *better late than never*. It is with this goal that lawyers, citizens and stakeholders promote the [amended] promulgation of the proposed Bill with due consideration and whilst keeping in mind the economic benefits that remote work could bring into Pakistan by virtue of

[2] The author has drafted a detailed consultation on the Bill for the Ministry of Information Technology and Telecommunications along with recommending amendments to find balance. It is yet to be seen whether such recommendations would be heard or whether the citizens of Pakistan will have to wait for another international quandary to push the legislative machinery into action. Available at: https://zflpg.zu.edu.pk/centre-for-law-and-technology/personal-data-protection/

potentially being allowed cross-border transfers of data from jurisdictions such as the European Union.

However, the law must necessarily be aligned with international best practices for it to be effective. The fundamental principles of personal data protection must be protected in the law without exception. It is yet to be seen whether these principles will be afforded the level of protection which is expected within the current contextual framework of personal data protection. As the Bill currently stands, as this paper shall explore, has many discrepancies pertaining to these very fundamental principles.

In order to explore and address these themes, the fundamental question which appears before us is – broadly – *with a specific focus on the fundamental principles of personal data protection, will Pakistan's proposed Personal Data Protection Bill, 2021, be effective and aligned with international best practices, once it is promulgated?* In order to attain more specificity in this endeavour, the author has dissected the primary question into three sub-questions:

1. What makes the right to privacy and personal data protection important in the digital age?
2. What are the fundamental principles of personal data protection according to international best practices?
3. Will the proposed personal data protection law effectuate the fundamental principles in its current form?

Once the abovementioned questions are answered and/or analysed, a conclusion may be drawn as to which amendments should be made to the proposed law to make it more effective.

Research Methodology

This paper utilizes qualitative research methods. In order to address the research and sub-research questions, prudently selected academic papers and books are utilised to establish- initially- the philosophical and logical arguments posited in support of the right to privacy and why it is important for this fundamental right to be protected in the specific context of the digital age. Jeremy Bentham's Panopticon shall be used as a case example on how the knowledge of (or knowledge of the potential of) surveillance alters human behaviour.

Next, a discussion on the importance of personal data protection shall be undertaken on the basis of the ever-evolving commercial-digital landscape of digital services *via* the internet. The principles of personal data protection elucidated in the European Union's General Data Protection Regulation, 2018, shall be examined with further reliance on material curated by European Union institutions. Once the importance of the right to privacy and the fundamentals of personal data protection have been established in the form of a working understanding, the author shall proceed to evaluate the proposed scheme of personal data protection in Pakistan in the form of the Personal Data Protection Bill, 2021, with a specific focus on its efficacy. Its salient provisions shall be juxtaposed against the protection afforded by the General Data Protection Regulation, 2018, and a comparative analysis shall be undertaken on the triumphs and shortcomings of the (proposed) law.

The analysis shall primarily be centred around the fundamental principles of personal data protection, the efficacy of the proposed law, and the potential loopholes which are either arbitrary/discretionary, not adequately transparent or leave room for *potential* abuse.

Finally, a conclusion shall be reached in which there shall be certain recommendations given insofar as amendments to the Personal Data Protection Bill, 2021, are concerned.

The Right to Privacy and Personal Data Protection

What makes the right to privacy and personal data protection important in the digital age?

The Right to Privacy

The fundamental right to privacy is enshrined in the Constitution of the Islamic Republic of Pakistan (1973) in Article 14, which reads as follows:

> *"14. Inviolability of dignity of man, etc.*
> *(1) The dignity of man and, subject to law, the privacy of home, shall be inviolable. …"* [emphasis supplied]

Although Article 14 posits the constitutional requirement to respect the right to privacy of citizens, a bare perusal of the wording

suggests that this right – insofar as Article 14(1) is concerned – is limited to protecting the privacy of a person's home. More broadly read, it could be inferred to relate to any residential premises. Furthermore, it is apparent that this is a qualified right (i.e. 'subject to law'). In effect, where the law permits (or rather, requires), the privacy of the home may be suspended. Notwithstanding the expansion of this right effectuated *via* case law, a protective regime solely based on this constitutional provision is severely inadequate for the ever-evolving needs of the contemporary era.

To proceed, it is imperative to understand the practical implications of the right to privacy. Let us consider the example of a person's personal (physical) space. Usually, one's room is their most immediate 'safe' space.[3] Their clothes, valuables, personal effects, items of sentimental value, art pieces, diaries & notebooks, books, and hobby-related items may be stored there with the expectation that they shall stay safe from prying eyes. It would not be out of place to suggest that no person can access this space and the items it contains without permission.[4] The fundamental reason for this barrier to accessing personal spaces and items to exist is to give credence and value to a person's discretionary authority, especially where it pertains to their private space.

An excerpt from Privacy International's explainer (2017) on what the right to privacy is, and why it is practically important is reproduced below, which serves as an effective contextual framework for approaching the topic:

> "Privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built.
>
> Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to

[3] 'Safe' in this context means a space where external interference is either negligible or non-existent without the consent of the person to whom that space pertains.

[4] Save for the exception provided: 'subject to law'. For instance, law enforcement agencies may execute a search and seizure operation in residential premises on the basis of an Order of the Court or on the suspicion of specific crimes being committed within the premises, provided that the relevant senior officer is present during the search.

interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information.

The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances.

As a result, privacy is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control.

Privacy is essential to who we are as human beings, and we make decisions about it every single day. It gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us."

The extrapolations that can safely be made from this excerpt highlight and codify most of the prominent (practical) reasons to support the right to privacy. Foremost in this list is the idea that each person has – or at least ought to have – the right to make autonomous decisions on the type and magnitude of visibility into their affairs. Akin to how we create social and psychological boundaries contingent on where we are and with whom we are associated in that environment,[5] the same sort of tiered-protection ought to be extended to be more aligned with the emergence of digital – rather than only physical – spaces.

This enhanced view of the right to privacy does more than simply ensure that personal spaces are protected: it ensures that personal data and information relating to a person which they would prefer to keep private, is protected. This protection of personal spaces and information has far-reaching effects: not only does it help maintain social boundaries and build trust between citizens and the state, but it also ensures that there is room for free political discourse without having to reveal one's identity.[6] It is an established principle that a society which has mechanisms for discourse is indubitably

[5] For instance, we are slightly 'different' versions of ourselves depending on where we are- for instance, reserved and professional at work, relaxed and informal in a social setting, and even more so at home.

[6] Such as having a pseudonym-based social media handle, which is used to engage in political discourse without having the untoward effects of political inclinations being held against the user.

better-equipped to deal with emerging problems rather than a society that tends to shun dissenting views.

Ever since the massive propagation of digital technologies and the increasing use of digital services, people have begun interacting with their machines (and services) in a manner similar to the intimacy of maintaining a personal diary. Web searches, research, interest-based web surfing, social media presence, formation (and propagation) of opinions, and entertainment are only a few common use-case examples of digital services. However, similar to how we conduct ourselves in our day-to-day lives (i.e. with a tiered system of visibility/insight into certain, select portions of our lives), this tiered mechanism of visibility/insight ought to be transferrable to one's digital spaces.[7]

Surveillance, Anonymity & Discourse

Jeremy Bentham wrote about the concept of the Panopticon (Bentham & Božovič, 1995) – a design for prisons to be built on a model that somewhat resembles a cylinder. At the very centre is where the guard tower stands, and at the circumference is where all the inmate's cells are present. The guard tower has one-way windows so in effect, prisoners cannot see the guards but the guards can see each cell, whenever they may choose to. As a result, the prisoners would not know *when* they are being directly observed, however, they know that they are potentially being watched at any given point in time. As a result of this thought, it was deduced that there is something about the nature of being surveilled that even if people are not being directly monitored but *think* they are being surveilled, they change their behaviour to be more socially palatable.

The right to privacy is perhaps one of the most relevant rights in the digital age, especially after the advent of mass-surveillance technologies such as the NSA's PRISM (Greenwald & MacAskill, 2017). The very knowledge of the existence of this program

[7] This claim can be easily exemplified with the following thought experiment: would you allow *all* of the following relations of yours to have *comprehensive* insight/visibility into your usage of digital services: your parent(s), your friend(s), your spouse(s), your child(ren), your boss, your colleague(s), your neighbour(s), and your enemy? The fact that most people would prefer a different level of insight for each of these categories of social and biological relations speaks to the veracity of the claim.

leaves very little to be said. Keeping in mind the psychological implications of the knowledge (or rather, potential) of being surveilled, digital surveillance may lead to one or both of the following:

i. The dilution (or self-censorship) of independent thought & discourse for fear of being identified as a troublemaker in the eyes of law enforcement agencies.
ii. The creation of deep web sub-cults in which participants enjoy a level of anonymity.

Lawrence Lessig, in his book *Code: version 2.0* (Lessig, 2006) gives the example of the University of Michigan undergraduate- Jake Baker. Jake was an unassuming fellow who one would easily forget, had they met him in a social setting for the first time. However, despite being so unassuming and rather mundane in real life, Jake had a large following online where he wrote and published short stories of a rather violent nature. The excessively graphic nature of his stories brought him into a sort of legendary popularity on the internet forum where he published his work. However, once his work was discovered by a Michigan University alum and it was seen that there was a Michigan University domain email address associated with the posts, the matter was brought to the attention of the police *via* the University, who promptly arrested Jake. In further investigations, it was discovered that Jake's stories were simply just words with no evidence to suggest that his graphic plots had any roots in reality. Nevertheless, the nature of his stories was enough grounds for concern by the University and anybody else who stumbled across them (besides the avid fans who read Jake's work zealously). The Courts held that Jake's words (by virtue of simply just being *words*) are protected by the First Amendment to the Constitution of the United States and that since there is no evidence to suggest that Jake had harmed another person, he was set free.

The Jake Baker debacle serves as an interesting point of discussion: Jake kept his 'deviant' persona limited to the internet and his sub-cult-like following of readers. His thoughts, graphic plotlines and literary works were never shared with people he knew at the University. It was only when his online work was inadvertently stumbled upon with the tag 'umich.edu' that the matter escalated into the notice of his 'real-world' associates. This

is arguably where the crux of the debate lies – whether Jake ought to be afforded the level of privacy to separate his two 'versions of being' (i.e. one being his online persona and one being his demeanour in the physical world). As discussed earlier, mostly all social actors have a tiered mechanism of visibility into certain aspects of their lives, which they alone choose. It is posited that the same discretionary choice ought to be granted to social actors online.

Let us consider an example that perhaps is more relatable to a resident of Pakistan. There are numerous accounts on Twitter which are run by people residing and working in Pakistan – sometimes even in notable (private) or official positions. However, some of these accounts are run under pseudonyms instead of the user's real name in order to remain anonymous. For some, the anonymity is an appropriate requirement by virtue of their position. For others, it is out of fear of untoward consequences Such as – inter alia – frivolous defamation suits. Nevertheless, it is observed that certain pseudonym-based accounts are deeply involved in discussions of a socio-political nature which are often not highlighted on media channels which fall under the regulatory umbrella of the Pakistan Electronic Media Regulatory Authority (PEMRA). Whether or not this is productive for Pakistan as a nation will be seen in due course, nevertheless, it is important for any society to be able to engage in free rational discourse without the fear of persecution or self-censorship on the basis of one's position in society. Philosophy and subjective truths must be allowed to surface for society to understand and regulate/update its 'collective consciousness' (Smith, 2014).

Thus far, we have discussed the importance of personal data protection from the context of surveillance and its psychological impact (self-censorship), from the context of a tiered-mechanism of insight into one's affairs, from the context of protection against persecution, and from the context of encouraging free socio-political discourse without undue inhibitions.

Personal Data Protection

To effectively protect the right to privacy in the digital age, the concept of personal data protection stands at the forefront as the first order of business in order to regulate the collection, processing,

inference-based decision making and/or any other use of data pertaining to real people. The primary focus of personal data protection – as the phrase suggests – is on personal data. **Personal data comprises of any piece of information which – directly or indirectly – identifies a natural person, or, by virtue of that information, a natural person is identifiable**. These 'pieces' of information include – but are not limited to – a data subject's[8] name, phone number, identity documents, email address, internet protocol (IP) address, location data, address, photographs, *et cetera*. Furthermore, 'special categories' of personal data also exist which are considered to be even more sensitive in nature than 'normal' personal data. The data points included in 'special categories' of personal data include one's religious or philosophical beliefs, genetic and health data, trade union membership, biometric data and racial/ethnic origin data, among others. The reason for this distinction is that some personal data is more sensitive than other data insofar as the potential consequences of a data breach are concerned.[9] It is important to note that 'harm' is not a consideration in matters pertaining to personal data protection. The foundation is built upon the *potential consequences* which may arise, with a specific regard to avoid 'significant risks to the fundamental rights and freedoms' (Recital 51 - Protecting Sensitive Personal Data, n.d.) of data subjects.

The question follows suit: what would comprise a significant risk to the fundamental rights and freedoms of data subjects? While there are portions of personal data protection regimes which are arguably within the discretion of the Controller to make decisions,[10] the *general* rule is to allow the data subject to decide. Knowledge and consent on the part of the data subject lie at the heart of personal data protection laws.

[8] Data Subject: the identified or identifiable natural person to whom personal data pertains (in context).

[9] For instance, your name and email address being made public would not have consequences which are as potentially far-reaching as say, if your racial/ethnic origin and religious beliefs were made public.

[10] For instance, deciding what comprises 'legitimate interest', 'vital interest' and 'public interest' per Article 6 of the GDPR.

Principles of Personal Data Protection

To effectively study the fundamental principles of personal data protection, we will examine the European Union's General Data Protection Regulation, 2018, which is being applied since the 25th of May, 2018 (European Commission (Ed.), n.d.). Hereinafter referred to as the 'GDPR', the European Union's General Data Protection Regulation, 2018, sets the benchmark as the most comprehensive personal data protection law presently in force in any jurisdiction across the globe.

The concepts of informed consent, thorough knowledge, and quick data breach notifications lie at the heart of the GDPR. A very strict approach is taken to data protection since the importance and possible ramifications of a breach are largely understood by both the promulgators/regulators as well as the entities to whom it applies.

Lawful, Fair & Transparent

Article 5 of the GDPR elucidates these principles, which begin with the primary marker: processing[11] must be *lawful, fair and transparent*. This immediately begs the question – what comprises *lawful* processing?

The GDPR – in Article 6 – expands upon the elements which render processing *lawful*, which are listed below:

i. Consent of the data subject: The data subject's consent to have their personal data processed for a specified (set of) purpose(s);
ii. Contractual requirements: Either where processing personal data is necessary to fulfil the requirements of a contract, or where processing is necessary as a pre-cursor to entering into a contract;
iii. Legal obligation: The Controller is subject to a legal requirement to process data;

[11] Processing is defined in Article 4 (2) of the GDPR as '*any operation or set of operations which is performed on personal data … such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*'

iv. Protection of vital interests: processing is *necessary* in order to protect the vital interests of either the data subject or any other natural person;
v. Public interest: where processing is necessary for the execution of a task that must be carried out in the public interest;
vi. Legitimate interest: where processing is necessary to effectuate any legitimate interests pursued by the Controller or third party unless such interests are trumped by the fundamental rights or interests of the data subject, especially where the data subject is a minor.

On a bare perusal of the grounds of lawful processing, it can be deduced that the primary intention of the GDPR appears to be that Controllers must have a concrete basis for processing personal data. In the absence of such basis or grounds – for instance, in a jurisdiction such as Pakistan – Controllers are at liberty to process personal data according to their own commercial interests or putting it otherwise, in quite an arbitrary fashion. It is this arbitrariness that is the bane of any expectation of respecting an individual's right to privacy.

Purpose Limitation

Article 5 (1) (b) of the GDPR posits the principle of purpose limitation. It signifies that Controllers should have legitimate, clear and unambiguous purposes defined for their processing exercises and that personal data should be collected *only* to the extent that it is necessary for fulfilling the defined purposes. Once defined, the 'purpose' cannot be changed, with the exception of engaging in further processing for the purposes of scientific, historical or research in the public interest. Furthermore, any processing done for statistical purposes or archiving in the public interest is also permissible without breaching the principle of purpose limitation.

Data Minimisation

Article 5 (1) (c) posits the requirement of Data Minimisation. This concept entails that Controllers ought *only* to collect those data points which are strictly necessary for the defined

purpose(s). No personal data shall be collected which does not pertain to the defined purpose(s).[12]

Accuracy

According to Article 5 (1) (d), Controllers must ensure that the data collected from a data subject for a specified, legitimate purpose, is accurate and where necessary, up-to-date. Where the dataset's utility has lapsed, it must be deleted without delay.

Storage Limitation

With the exception of scientific research, statistical data in the public interest, and historical or research in the public interest, all personal data must be erased as soon as the purpose for which it was collected has been completed. It is pertinent to note, however, that the exceptions listed herein are subject to the Controller implementing adequate and effective technical and organisational measures to ensure the safety of the personal data. The principle of storage limitation is elucidated in Article 5 (1) (e) of the GDPR.

Integrity & Confidentiality

As a general and wide-arching obligation, Controllers must ensure that all processing endeavours are subject to protection against unlawful use, access, loss, damage and/or destruction by way of implementing adequate and effective organisational and technical safeguards. Article 5 (1) (f) of the GDPR lays down this requirement, with its primary focus on the security of personal data, and the onus of which lies with the Controller.

Pakistan's Personal Data Protection Bill, 2021

In 2018, the Ministry of Information Technology & Telecommunications (hereinafter referred to as 'MoITT') drafted the first iteration of the Personal Data Protection Bill (2018) and

[12] For instance, for a food delivery app, the only information required to execute the contract/deliver the service is your name, address, phone number and payment details. Additional data such as your IP address, ID, photograph, etc. are not strictly necessary for the defined purposes.

opened the same for public consultation. Subsequently, MoITT amended the draft to incorporate what can be assumed to be industry recommendations and issued the Personal Data Protection Bill (2020) as amended for public consultation. After doing the consultation and amendment exercise once more, the MoITT has uploaded the latest version of the Personal Data Protection Bill, 2021 (Consultation Draft, 2021). The government of the Pakistan Tehreek-e-Insaf had given its approval to the bill *via* the Cabinet, which was meant to be escalated to the National Assembly and subsequently, the Senate, to gain the status of an Act of parliament (if assented to by both houses). However, following the vote of no confidence against the erstwhile Prime Minister, the incumbent government reverted the former Cabinet's approval, thus reverting the bill back to the pre-Cabinet-approval stage.

Legislative Latency

Historically, Pakistan has lagged behind the contemporary world in matters pertaining to legislative action. For instance, while the United States promulgated the Computer Fraud and Abuse Act in 1986 and the United Kingdom promulgated the Computer Misuse Act in 1990, Pakistan followed suit with the Prevention of Electronic Crimes Act in 2016. Furthermore, our neighbours to the East promulgated the Geographical Indications of Goods (Registration and Protection) Act in 1999, which came into force in India in 2003, whilst Pakistan followed suit by way of the Geographical Indication (Registration and Protection) Act in 2020 – more than two decades later. The geographical indicators law posed a significant problem for Pakistan when India asserted its exclusive right to export *basmati* rice to the European Union (Jamal, 2020). The dispute between India and Pakistan goes back more than two decades; it would not be unreasonable to suggest that Pakistan could have promulgated effective legislation pertaining to geographical indications sooner than 2020. Moreover, whilst certain states promulgated legislation pertaining to the right to information as far back as 1966: for instance, the United States Freedom of Information Act, 1966; Pakistan's Right to Information Act was promulgated in 2013.

The examples are numerous – extending to topics including (but not limited to) child marriages, intellectual property rights,

environmental protection, anti-money laundering and counter-terrorism financing, climate change, women's rights, domestic violence, rights of marginalised communities, child labour, human trafficking, *et cetera*, which further exemplify the legislative latency that can be witnessed in Pakistan.

It can be argued that at present, perhaps the most pressing matter to be tended to is personal data protection. In the absence of a legislative regime, foreign tech corporations are apprehensive of working with Pakistan-based companies, specifically in terms of outsourcing information technology-related work which has a personal data component in them. As a result, Pakistan is not fully taking advantage of this potential stream of foreign exchange remittances – which appears to be the country's most wanted liquid asset. Therefore, it is not out of place to say that as a country, Pakistan cannot afford to be investing so much time into a critically-required piece of legislation.

Effective or Cosmetic Protection?

The Personal Data Protection Bill, 2021, (hereinafter referred to as the 'PDP Bill' or the 'Bill') attempts to stay as close to the fundamental principles of personal data protection as are laid out in the GDPR, however, there are certain deficiencies which are immediately visible upon a thorough analysis of the proposed law.

Although there are provisions in the Bill that attempt to codify the fundamental principles of personal data protection, the exceptions created within the provisions tend to leave large loopholes – essentially rendering the Bill *just short* of ineffective. Furthermore, as a general comment, the Bill is not drafted with the same degree of clarity as the GDPR. This not only makes it difficult to compare – point by point – how effectively the fundamental principles are codified, but will inevitably add to the conceptual confusion which is bound to plague the very people who will be tasked with enforcing the law, once it is passed.

Consent & Exceptions Thereto. Section 5 (1)[13] of the Bill imputes the requirement of consent from the data subject for the

[13] *"5 (1) A data controller shall not process personal data including sensitive personal data of a data subject unless the data subject has given his consent to*

processing of their personal data. This provision is highly effective, aligned with international best practices, and encourages trust-building between data subjects and controllers. However, in section 5 (2)[14], the exceptions to consent are elucidated, which include – *inter alia* – two potentially problematic stipulations: The Controller may continue processing personal data in order to protect the 'vital interests' of the data subject, or where such processing falls within the 'legitimate interests' of the controller.

According to section 2 of the Bill, the definition of 'vital interests' includes matters pertaining to fundamental rights, security of data subject(s), humanitarian emergencies, disasters and management/monitoring of epidemics. This is a cause for concern since effectively, any protection afforded to data subjects under the Bill would be held in abeyance if it is held that a matter falls within the ambit of one of the paradigms listed above. It is presumably the discretion of the proposed National Commission for Personal Data Protection (hereinafter referred to as the 'Commission') to decide when to suspend the operation of the provisions in order to protect 'vital interests'. The Bill vaguely touches upon the aspect of transparency in sections 33 (2) (e)[15] and 34 (2) (c) (ii)[16], however, it

---

the processing of the personal data. A separate consent shall be obtained from the data subject for each purpose."

[14] *"5 (2) Notwithstanding sub-section (1), a data controller may process personal data about a data subject if the processing is necessary for either of the following:*

…

(c) in order to protect the vital interests of the data subject;

…

(e) for legitimate interests pursued by the data controller; …"

[15] *"33 (2) Without prejudice to the generality of the foregoing and other functions set out under this Act, the Commission shall particularly perform the following functions:*

…

(e) ensuring that all of its decisions are based on established principles to structure or minimize discretion and ensure transparency and accountability …"

[16] *"34 (2) In particular and without prejudice to the generality of the foregoing power, the Commission shall:*

…

(c) formulate compliance framework for monitoring and enforcement in order to ensure transparency and accountability, subject to the measures including but not limited to the following:

…

(ii) . Transparency …"

is not guaranteed for the decision-making processes to be made transparent or as a result, justiciable.

The more problematic of the two exceptions is the 'legitimate interests' exception. Controllers are allowed to – in the absence of consent – continue processing personal data where they are pursuing a legitimate interest. The Bill defines legitimate interest as '*anything permitted under the law'*. It is at this juncture that the author would like to posit the argument that such a wide-spanning exception effectively desecrates any protection offered by the Bill. Let us consider the following example:

> Arsalan goes to a clothing store and purchases Eid clothes for himself and his family. At the checkout counter, he is asked for his name, email address and phone number. The reason given to him is that the personal data is required in case they need to intimate him about him winning a prize out of their ongoing lucky draw, or to reach out to him if there is a promotional offer they think he might be interested in, or to collect customer points which he can then redeem later on for goods. In this scenario, Arsalan would be deemed to have consented to such processing by way of affirmative action (he provided the personal data at the counter). Furthermore, the clothing store will also have mentioned the purpose for which the data is being collected. However, in the event that Arsalan revokes his consent as per section 23 of the Bill, the clothing store will still not be strictly required to cease all processing, since, effectively, they can rely on section 5 (2) (e) and argue that their legitimate interest is in consolidating customer data and selling it to marketing agencies along with a general (value-addition) estimate of their buying power. The argument can be further buttressed by the fact that this purpose has existed since the time of collecting the data and that nothing in the Bill explicitly disallows processing done lawfully.

Technically speaking, the argument appears to have merit. It can quite effectively be argued that a commercial entity's legitimate interest revolves around commerce and profit-making. Since accurate personal data is sold at a premium to marketing concerns, the exercise by the hypothetical clothing company in the example above may be portrayed as a legitimate business opportunity that

they routinely pursue as a revenue source for the company. Bearing in mind that 'legitimate interest' is defined as anything permitted by law, there does not seem to be an explicit bar to such an argument.

Purpose Limitation & Data Minimisation. Section 4 (2)[17] of the Bill successfully and efficiently codifies the principles of purpose limitation and data minimisation, in addition to section 5, subsection 3[18]. However, insofar as purpose limitation is concerned, there are far too many exceptions which may be used/abused to sidestep the intention behind the provisions. Consider the argument posited hereinabove in 3.2.1 integral hereto. Moreover, section 24 stands as a paradoxical clause, effectively destroying the concept of purpose limitation. We shall examine the effects of section 24 in the next portion of this paper.

Integrity & Confidentiality. There is a general requirement that personal data shall not be disclosed to any party[19] without the consent of the data subject. Knowledge of the data subject appears to be the primary focus, however, the general requirement in section 7[20] is subject to section 24 of the Bill. The exceptions listed in section 24 are perhaps the most concerning provisions in the entire Bill. It reads as follows:

> *"24. EXTENT OF DISCLOSURE OF PERSONAL DATA*
> *Notwithstanding section 7, the personal data of a data subject may be disclosed by a data controller for any purpose other than the purpose for which the personal*

---

[17] *"4 (2) The data be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed."*

[18] *"5 (3) Personal data shall not be processed unless:*
a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;
b) the processing of the personal data is necessary for or directly related to that purpose; and
c) the personal data is adequate but not excessive in relation to that purpose."

[19] Exceptions exist, for instance, a class of third parties with which the Controller shall share personal data with, provided that a written notice has been sent to the data subject. See: section 6 (1) (e) of the Bill.

[20] *"7 (1) Subject to section 24, no personal data shall, without the consent of the data subject, be disclosed …"*

> *data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:*
> *a) the data subject has given his consent to the disclosure;*
> *b) the disclosure —*
>
> *i. is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or*
>
> *ii. was required or authorized by or under any law or by the order of a court;*
>
> *c) the data controller acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;*
> *d) the data controller acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or*
> *e) the disclosure was justified as being in the public interest in circumstances as determined by the Commission in advance of the disclosure.*" [emphasis supplied]

At a bare perusal of the wording of section 24, it is immediately apparent that there are far too many loopholes in this proposed data protection regime. It is important to bear in mind that the section creates an exception to the general rule that personal data shall not be disclosed without consent, or at the very least, without the data subject's knowledge. Not only this but the fundamental principle of purpose limitation has also been desecrated since this provision applies to the disclosure of data for purposes *'other than the purpose for which the personal data was to be disclosed at the time of its collection'*. The draftspersons have attempted to limit the desecration (of protective measures) by adding conditions to be fulfilled in order to avail the exception created by the section, however, this has only made matters worse. In proviso (c) and (d), the standard of judgment to create such a huge exception (i.e. waiving the requirement of consent, and also disclosing data to fulfil a purpose, *regardless* of whether that purpose existed at the time of collecting the personal data) is the Controller's 'reasonable belief'. Proviso (c) posits the weak standard of a Controller having a *reasonable belief* that he or she had the right under the law to

disclose the data. It is put to the authorities that not all Controllers will necessarily be well-versed in the law. Furthermore, the placement of a data protection officer is vague and undefined. There seems to be a provision for the existence[21] of the data protection officer, however, it is not codified whether a data protection officer will be a standard requirement for Controllers of all magnitudes, or not. Based on these ambiguities alone, the Bill will not win the confidence of data subjects or privacy lawyers.

Nevertheless, the more problematic proviso pertaining to the weak standard of reasonable belief is subsection (d) of section 24. The Controller may disclose personal data where they have a reasonable belief that the data subject would have consented to the disclosure, had they known of it and the circumstances surrounding it. Granted, this provision may act as a fail-safe in the absence of the data subject, however, it creates massive room for abuse. Since a subjective standard like 'reasonable belief' cannot be judged with any degree of specific accuracy, it leaves much undefined and as a result, chips away at the data subjects' trust. One cannot know the facts and circumstances of an individual. This proviso depersonalizes data subjects and proceeds with the assumption that decisions can be made on behalf of the data subject without their knowledge or consent. This is in stark contravention to the very philosophy of personal data protection and renders the protection afforded in the Bill all but redundant. For a personal data protection scheme to be holistically successful and effective, it is required that each data subject be perceived and treated as an individual, with unique goals, aims, problems and social positioning. It is firmly posited that especially in Pakistan – where the element of reasonableness may or may not be effectively present in the thought processes of all persons – it would be better to err on the side of caution than to extend discretionary decision-making authority to the Controller. Each data subject ought to be adequately informed

[21] Section 13 (3): *"The personal data breach notification shall at least provide the following information: -*
… (c) name and contact details of the data protection officer or other contact point where more information can be obtained …" See also: section 34 (2) (c) (viii) where it is stated that the Commission shall formulate a compliance framework for monitoring and enforcement in order to ensure transparency and accountability, subject to measures including … the responsibilities of a data protection officer.

and consent ought to be sought prior to proceeding with the disclosure of data, whether or not the Controller reasonably believes that the data subject would consent to such disclosure: the final authority in such matters must necessarily remain with the data subject.

Leaving the worst for last – a disclosure made for the purpose of *detecting* a crime is rather wide-spanning. This can mean, for instance, that there is absolutely no basis required for law enforcement agencies or regulatory authorities to request access to personal data. Granted, it is imperative to let these agencies and authorities do their work effectively to ensure the safety and security of residents, however, allowing such wide-spanning arbitrary powers defeats the purpose of the Bill and may even fall under the ambit of what is colloquio-legally called a 'fishing expedition' in which law enforcement agencies or regulatory authorities – without any grounds to justify suspicion – can dig into the affairs of entities to seek out discrepancies. The law generally affords protection against such 'fishing expeditions' and the same should not be allowed *via* this Bill.

Storage Limitation & Accuracy. The Bill effectively and holistically covers the fundamental principles of storage limitation in section 9[22] and accuracy in section 10.[23] The only cause for concern is the last line of section 10 (2) which reads that data subjects can access and rectify their (inaccurate or out of date) personal data '*except where compliance with such a request to such*

[22] *"9 (1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose or as required under the law.*
(2) It shall be the duty of a data controller to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed or as required under sub-section (1)."

[23] *"10 (1) A data controller shall take adequate steps to ensure that the required personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.*
(2) A data subject shall be given access to his personal data held by a data controller and data controller be liable to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act."

access or correction is refused under this Act.' This provision has the *potential* to be abused, however, such abuse will only manifest once the Commission is formed and it forms rules under the Bill once it attains the status of an Act. It is not necessary that it be abused; the author is re-iterating the *potential* for abuse, which is better to be isolated and rectified before it has the chance to manifest.

Controller's Liability. In the form of sections 8 (3) and 8 (4) we discover another potentially problematic mechanism, this time relevant not just to personal data, but rather to the attribution of responsibility and liability.[24] Per section 8 (3), the Controller, in the event that they are appointing a Processor on their behalf, must only ensure that the Processor undertakes to implement the security mechanisms required under the proposed law. Section 8 (4) further exacerbates the issue by making the Processor independently liable for the steps they are required to take with respect to ensuring adequate safety and security of personal data.

Although imputing responsibility and liability on the Processor is not out of place, the problem arises when the Controller's responsibility and liability could potentially be diluted as a result of these provisions. The Controller is the entity which is meant to be responsible for – *inter alia* – personal data processing, security and integrity. It is therefore the responsibility of the Controller to ensure that if they are opting to outsource their processing works, to engage an entity which is reliable and is either already implementing the security mechanisms, or demonstrates – to the satisfaction of the Controller – that they have implemented the requisite mechanisms in order to be able to undertake the processing works on behalf of the Controller. In a nutshell, it is the position of the author that section 8 (4) ought to be rephrased to reflect that the Controller and

[24] *"8 (3) Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall, for the purpose of protecting the personal data in the terms mentioned at sub-section (1)* ***ensure that the data processor undertakes to adopt applicable technical and organizational security international standards*** *governing processing of personal data, as prescribed by the Commission.*
8 (4) The data processor is ***independently liable*** *to take steps to ensure compliance with security standards prescribed under sub-section (1)."* [emphasis supplied]

Processor are jointly *and* severally liable for any personal data breaches.

Conclusion & Recommendations

The Personal Data Protection Bill, 2021, as it currently stands, requires significant amendments. The principles of informed consent, purpose limitation and integrity & confidentiality must necessarily be enhanced to afford actual, practical protection rather than a cosmetic, *prima facie* protection regime. The exceptions created to these principles must be removed and a holistic trustworthy law ought to be enacted. Granted, there are numerous commercial and legal considerations of future Controllers to oppose such amendments, however, in order to be contemporarily relevant, to be able to do business with foreign jurisdictions, and to gain the trust of data subjects, it is necessary for the Bill to be amended in light of the foregoing. Most of the recommendations have been incorporated into the relevant portions of this paper, however, for the ease of understanding of readers, the author has drawn up the following table with the most important amendments to be made in the Bill. It is pertinent to note that this list is not exhaustive and that this paper has been mainly restricted to the fundamental principles of personal data protection and not the entire personal data protection regime.

Issue	Recommendation
Definition and application of the concept of 'Vital interests'	Ought to be properly defined, with a transparent mechanism as to the considerations whilst deciding on vital interests. Humanitarian emergencies and the management of epidemics needs to be struck off completely and replaced with an anonymised dataset-based mechanism of study. Identifiable personal data need not be utilised to study the spread of epidemics.
Definition and application of the concept of 'Legitimate interests'	Ought to either be struck off completely, or severely restricted, along with a requirement of mandatory consent of the data subject, unless such consent has been gained at the time of collecting personal data.

The fundamental principle of Purpose Limitation is ineffective due mainly to the operation of S.24 of the Bill. The same section also strikes at the principle of Integrity & Confidentiality	Prevention, detection and investigation of crimes ought either to be completely struck off as grounds for seeking access to personal data unless such access is: i. Ordered by a Court of Law, ii. An investigation pertaining to a registered criminal case, or, iii. In pursuit of preventing a known crime. Nothing in this section should be phrased to the effect of allowing 'fishing expeditions'; there must be sufficient grounds to seek access *prior* to accessing the personal data
Transparency requirements seem to be inefficient	The functioning of the Commission and its decision-making generally has a transparency recommendation; however, it is recommended that such a principle be strongly and clearly codified in the Bill to enhance trust
Controller's Liability	The Controller and Processor ought to be jointly and severally liable; it ought to be the Controller's responsibility to ensure that the Processor they engage is up to par and abiding by the provisions of the law

References

Abdullah, O., Bashir, S., & Ali, R. N. (2023). The potential geographical indications in Pakistan. *Winter 2023, 3*(1), 335-346. doi:10.54183/jssr.v3i1.154

Amin, T. (2023, April 07). Draft data protection bill does not address industry's major concerns, claims AIC. Retrieved April 10, 2023, from https://www.brecorder.com/news/40235901

Bentham, J., & Božovič, M. (2011). *The Panopticon Writings*. London: Verso Books.

Editorial. (2021, June 09). Basmati dispute. Retrieved April 10, 2023, from https://www.dawn.com/news/1628365

European Commission (Ed.). (n.d.). Data protection in the EU. Retrieved April 10, 2023, from https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en#:~:text=The%20General%20Data%20Protection%20Regulation%20(GDPR),-Regulation%20(EU)%202016&text=A%20single%20law%20will%20also,applies%20since%2025%20May%202018.

Greenwald, G., Poitras, L., & MacAskill, E. (2013, June 07). NSA PRISM Program taps into user data of Apple, Google and others. Retrieved April 10, 2023, from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hoofnagle, C. J., Van der Sloot, B., & Borgesius, F. Z. (2019). The European Union General Data Protection Regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98. doi:10.1080/13600834.2019.1573501

Jamal, N. (2020, October 4). *Footprints: Basmati battle*. DAWN.COM. https://www.dawn.com/news/1583144

Kuneva, M. (2009). Meglena Kuneva - European Consumer Commissioner - Keynote Speech - Roundtable on Online Data Collection, Targeting and Profiling. Retrieved April 10, 2023, from https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156

Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books.

Ministry of Information Technology & Telecommunication. (Personal Data Protection Bill, 2021, Consultation Draft V.25.08.2021). Retrieved April 1, 2023, from

https://www.moitt.gov.pk/SiteImage/Misc/files/25821%20DPA%20Bill%20Consultation%20Draft_docx.pdf

Privacy International. (n.d.). What is privacy? | privacy international. Retrieved April 10, 2023, from https://www.privacyinternational.org/explainer/56/what-privacy

Privacy International. (2017, October 23). What Is Privacy? Retrieved April 10, 2023, from https://www.privacyinternational.org/explainer/56/what-privacy

Recital 51 - Protecting Sensitive Personal Data. (n.d.). General Data Protection Regulation (GDPR). https://gdpr-info.eu/recitals/no-51/

Smith, K. (2014). *Émile Durkheim and the collective consciousness of society: A study in criminology*. London: Anthem Press.

The Constitution of Pakistan (1973). Retrieved from https://www.pakistani.org/pakistan/constitution/

The Newspaper's Staff Reporter; Dawn. (2021, March 21). 'more transparency needed in Personal Data Protection bill'. Retrieved April 10, 2023, from https://www.dawn.com/news/1613664/more-transparency-needed-in-personal-data-protection-bill

The Correspondent; The Express Tribune. (2021, March 21). 'extremely serious situation in Pakistan'. Retrieved April 10, 2023, from https://tribune.com.pk/story/2290551/extremely-serious-situation-in-pakistan