BOLO BHI
Advocacy - Policy - Research

Bolo Bhi's Analysis of the Personal Data Protection Bill 2020

On April 10, 2020, the Ministry of Information and Technology and Telecommunications (MOITT) invited input from stakeholders on a draft Personal Data Protection Bill 2020 via email by May 15, 2020. Putting up a draft seeking stakeholder input is certainly a good step towards transparency and a collaborative, consultative process, unlike the approach adopted with the Citizens Protection (Against Online Harm) Rules 2020 – the status of which is still unclear following Federal Cabinet approval.

Drafts of data protection bills have been under discussion since 2005 in Pakistan. Several versions have surfaced under different governments. The protection of citizens' data is long overdue and legislation seeking to extend safeguards is necessary. However, the current draft does not adequately extend safeguards to citizens and, like the Prevention of Electronic Crimes Act (PECA) 2016 and Citizens Protection (Against Online Harm) Rules 2020, the bill awards discretionary powers which will lead to weak accountability and likely privacy violations of citizens' communications and, in turn, a chilling effect on speech. Some of this is explained further in the analysis below, which deals with some of the major concerns.

Pakistan, like the rest of the world, is currently grappling with a pandemic. Around the world and here, governments have deployed technology to trace, track and surveil citizens citing these as COVID-19 measures. However, concerns about such measures going beyond just dealing with COVID-19 exist and are not misplaced. In light of this, any legislation proposed during this time should not be rushed.

Review and revision of the bill and consultations on it must remain ongoing. Rushing the PECA 2016 was a mistake and evidence of it is abundantly available and visible. The same must not be repeated with this bill. Nor should COVID-19 be used as an excuse to legislate via Ordinance. The Citizens Protection Against Online Harms Rules 2020 should also be kept separate from this process. The draft Personal Data Protection Bill 2020 merits a discussion while the Citizens' Protection Against Online Harms Rules 2020 should only be discarded.

BOLO BHI
Advocacy - Policy - Research

Overview of Analysis on the Personal Data Protection Bill 2020

Vague definitions: Definitions are vague and there is no distinction or categorization between individuals, public, and private sector, personal or commercial use with respect to data controllers and processors. Vague and undefined terms, left to interpretation or to be defined after the enactment of the legislation, also provide no clarity or certainty in terms of responsibilities, liabilities, or protections.

Absence of Clear Procedures and Guidelines and Lack of Clarity on Responsibility/Liability: The bill must detail procedures and be accompanied by detailed illustrations and guidelines that enable all those who fall under the definition of data controllers and processors to fully understand what is expected of them and the liability placed so they may structure operations accordingly. Scale and nature of operations must also be taken into account given the ability of a person, small organization, large corporation, or government entity to collect and process data. Government-run public bodies should be explicitly mentioned in the bill considering the vast amount of data they process and leaks/hacks having taken place in the past.

Broad, Discretionary Powers and Penalties: The Federal Government is allowed to grant or revoke exemptions to any data controller which is completely arbitrary, there is no process prescribed, it is to be done through an executive process devoid of any checks and balances. This is also prone to political influence. The Authority has also been awarded powers of a civil court without any prescribed limits on powers or parameters within which they are to be exercised, nor what in the event of a violation or misuse. It can summon information and impose fines in the millions, however the procedure to do this is not prescribed.

Lack of Independent Oversight and Accountability: Authority set up under this Act is not autonomous or independent and functions under the Federal Government administratively. The Federal Government also appoints members – one of them an ex-officio member of a Ministry. They function as employees of the Authority. Salaries are paid through a Fund set up and money contributed by the Federal Government. The

Authority is also permitted to seek foreign aid and make investments without any parameters and constraints, which may lead to conflict of interest and no process on how to resolve this.

Data Localization: The bill allows the Authority to come up with a mechanism that requires a "copy of personal data" to be kept in Pakistan. Other than the monetary costs attached to doing this, there are grave privacy concerns. To whom will this data be provided to store, process, protect, and access? For what purpose? The Authority is not independent and functions under the Federal Government and most likely will result in a regime much like the Citizens Protection (Against Online Harms) Rules 2020. Practically getting intermediaries to follow through with a requirement such as this legally and practically will pose its own challenges.

Clause-wise Commentary

2(a) data subject	is a "natural person" but this is not defined just as in PECA 2016, where this is found and presumed to apply to an individual vs a legal entity which is covered under the definition of a "person." However, while individuals are data subjects, in various instances, so are private sector organizations for instance, in relation to public sector institutions such as regulatory bodies. Confidential organizational data is shared for the purpose of audits, compliance etc. Control and processing of such data should also be accounted for.
2(b) Personal Data	**"**any information" should be further categorized and defined. The definition in the draft is too vague and 'information' itself is undefined. If it has the same meaning as in other Acts such as PECA, that needs to be specified here.

2(c) Data Controller & 2(d)Data Processor	There should be clear distinction between state authorities, commercial entities, other legal entities, and individuals especially when with respect to responsibilities, liabilities, and penalties.
2(n) Vital Interests	“Matters relating to life, death and security” is very broad, this needs to be qualified further.
2(o) Authority & Critical Personal Data	Similar to critical infrastructure in PECA 2016, which has still not been designated by the Federal Government as required by the Act, “critical personal data” is to be classified by the Federal Government as per the bill. However, while there exists a definition of critical infrastructure in PECA 2016, there is none here. This must be defined and separated from the definition of Authority.
3 Scope and Applicability	The bill seeks to extend jurisdiction over those who may not be present or legally incorporated in Pakistan, but control or process data with respect to data subjects as defined in this bill. Section 3.2 requires such an entity - likely to apply to intermediaries and social media companies - to “ nominate for the purposes of this Act a representative.” The word used is “shall” so this is not optional. However, whether this will be accepted practically remains to be seen, as well as the legality of its application. Nowhere is there any specific reference to this bill extending this to public sector institutions which hold, process and share data of citizens. It would appear that Section 3.3(d) covers them. However, given some of the most confidential data is in the possession of public sector institutions, and many breaches and violations occur, a

	sub-section should be added to specifically cover them so there is no ambiguity.
4 Protection of Personal Data	This only mentions “personal data” whereas the definitions section lists and defines “anonymized data,” “sensitive personal data,” and “critical sensitive data” separately. Therefore it should be made clear if these are being excluded in this section and if so, why. Otherwise these definitions should also be listed here so there is no ambiguity regarding what this section extends to.
Section 5 General Requirements	Section 5.1 requires consent to be given in order for data to be processed, however it is silent on how this consent is to be acquired. The definition of consent includes a qualification which should be included here and the process should be detailed to set a baseline requirement to safeguard a data subject. Each time data is to be obtained, processed or shared for a different purpose, consent should be explicitly obtained. Section 5.2 allows the data controller to process data if the processing is necessary and in the list provided on when it may be necessary are Section 5.2(d) “in order to protect the *vital interests* of the data subject” and Section 5.2(f) “for *legitimate interests* pursued by the data controller.” The terms “vital interests” and “legitimate interests” are undefined, broad and leave it up to the data controller and processor to decide arbitrarily. There should be guidelines for whether a data processor or controller can and should even decide this.
6 Notice to the Data Subject	With respect to the data notice that is to be provided to the data subject, Section 6.2 states “as soon as reasonably possible.”

	If a timeframe cannot be fixed - however this should be discussed during consultations - then an upper limit must be set. It should not be left open ended as this or defeats the very purpose. There should also be a subsection dealing with failure to provide notice to data subject, either at all or within the prescribed time frame and the remedy available to a data subject.
8 Security Requirements	Due to the technical nature of this bill, proposed Rules, guidelines, illustrations and appendices should be prepared and shared along with the bill for greater clarity so it is easy for those to whom this applies to discern the level of compliance required and liability placed on them, to start thinking ahead.
9 Data Retention Requirements	Section 9.1 states the data "shall not be kept *longer than is necessary*" which is again vague and open-ended. At least an upper limit should be prescribed and during consultations what may be a reasonable window should be discussed. When data is destroyed or permanently destroyed as required by Section 9.2, the data subject should be informed in writing using the same process in Section 6.
10 Data Integrity and Access to Data	How this is to be done should be specified in the form of some guidelines. Under Section 10.2 where a data subject is granted access to his/her personal data unless refused to meet compliance requirements under the Act, a process should be outlined for this where the request and refusal is recorded and the refusal is explained in writing and

	provided to the data subject who should also have a right to contest/appeal this.
11 Record to be Kept by Data Controller	Instead of leaving it to the discretion of the Authority how the record is to be maintained as per Section 11.2, this should be specified in the law itself.
12 Transfer of Personal Data	How is authorization decided or to be verified needs to be explained.
13 Personal Data Breach Notification	Section 13.1 requires a data controller to notify the Authority within 72 hours in case of a breach "except where the personal data breach is *unlikely to result in a risk to the rights and freedoms* of the data subject." This is a very subjective and arbitrary decision which the data controller should not unilaterally be able make and certainly not without qualification, guidelines, and parameters, which should be defined in the law. Section 13.2 requires the data controller to explain to the Authority if a breach is not reported within 72 hours as required by Section 13.1. Both the notification and reasons for delay if such is the case, should also be provided to the data subject. The data subject, is unsatisfied with the reasons provided by the data controller, should have the right to lodge a complaint with the Authority, the procedure for which should be defined, including penalties.
14 Cross Border Transfer of Personal Data	How will this be implemented with respect to social media platforms and other intermediaries whose email services, social media applications, cloud storage facilities etc are used by citizens in Pakistan but are not present in Pakistan?

	Section 14.1 states “critical personal data shall only be processed in a server or data centre located in Pakistan.” Critical personal data must be defined in the law so there is clarity on what it is. This will also mean setting up the mechanisms required to do so. What amount of citizens’ data qualifies as this or “sensitive personal data.” Citizens should know what from among their data falls under these categories, their access to it and the limitations on its use so that those responsible for controlling and processing it are aware of the limits.
15 Framework on Conditions For Cross-Border Transfer of Personal Data	Section 15.1 leaves it to the discretion of the Authority when and how personal data may be transferred outside of Pakistan. Section 15.2 requires a “copy of personal data” to be kept in Pakistan. This is an attempt at data localization. Other than the monetary costs attached to doing this, there are grave privacy concerns. To whom will this data be provided to store, process, protect and access? For what purpose? This should not be attempted at all. The Authority is not independent and functions under the Federal Government and most likely will result in a regime much like the Citizens Protection (Against Online Harms) Rules 2020.
31 Power To Make Further Exemptions	This section is too vague and awards overbroad and discretionary powers to the Federal Government and the Authority. Section 31.1 allows the Federal Government to “exempt the application of any provision of this Act to any data

	controller" by an order published in the official Gazette. Section 31.2 allows the Federal Government to "impose any terms or conditions it thinks fit in respect of any exemption." Section 31.3 allows the Federal Government to "revoke any order made under subsection(1)...at any time." All of this is completely arbitrary and not subjected to any process or checks and balances. Vesting these powers in the Federal Government will also make this prone to political influence which will result in picking and choosing who to exempt. The bill must be applicable to all equally and guidelines and processes should be clearly defined in it. If an exemption is to be granted, there should be a prescribed procedure in the bill whereby a request in writing is made by a data controller stating reasons, which is placed before an independent authority – which this Authority or the Federal Government is not. Any exemption granted on the basis of this request should be recorded and supported with reason, and an objection against a conflict of interest raised by any other party should lie before court.
32 Establishment of the Authority	Section 32.1 grants the Federal Government the power to establish the Authority. Such a body should be constituted under this Act as a statutory body. Earlier versions of the bill set up a commission which is what should be done. Section 32.2 states "The Authority shall be an autonomous body under the administrative control of the Federal Government." The Authority cannot be autonomous if it is under the administrative control of the Federal Government. Even regulatory bodies such as PTA and PEMRA, set up by Acts of Parliament suffer for control and influence and are not completely free though they

	should be independent regulators. This Authority will have far less autonomy and independence than even them. Section 32.4 The composition of the Authority is very similar to what was attempted when the Inter-Ministerial Committee for the Evaluation of Websites (IMCEW) was set up in 2006 by an executive order of the then Prime Minister. The appointments for the Authority are to be made by the Federal Government. Rather it should be an independent commission with parliamentary oversight and follow an appointment process independent of solely government approval. Section 32.4(a) appoints at least one ex-officio member who is to be a member of the Ministry of IT and Telecom, Ministry of Defence or Ministry of Interior. This compromises the ability of the committee to conduct across the board accountability, especially of those in the public sector. Section 32.4(b) lists four sectors from which other members must be appointed, who will essentially serve as employees of the Authority. This in effect makes them employees of the Federal Government especially when salaries will be paid from money given to the Fund set up under Chapter 6 Section 40 and the Authority operates under the administrative control of the Federal Government.
34 Powers of the Authority	The Authority has been given powers of a civil court yet how they may be exercised and the parameters within which this must be done is not explained in the bill. The Authority has been given the powers to impose penalties but no process prescribed. What right of hearing is available, how is it to be decided, none of this is clear.
36 Power of the Authority to Call for	Under what circumstances would the Authority require information from a data controller or processor for the

Information	discharge of its functions? This needs to be clarified. While Section 36.2 requires the Authority to provide this in writing, once the data or information is handed over, what are the procedures in place to maintain integrity, safety, confidentiality. What are the permissible ways it may be used and if there is a violation what is the mechanism for accountability, none of which is present in this section.
41 Submissions of Yearly Reports, Returns etc	These reports should be tabled before parliament and there should also be a penalty for not meeting requirements under this section of the law. FIA has been known to flout the mandatory provision in PECA which requires it to present bi-annual reports to parliament however it has only done so once since the enactment of the law in August 2016. The number here on in the bill also needs to be fixed as the number 41 appears again in other chapters of the bill.
Chapter 7 Complaint and Offences	Sections 41, 42 and 43 prescribe penalties, fines for which go up to millions of rupees. A lower limit should also be prescribed. Some categorization based on type of offence or violation under the Act and scale of operation – whether individual, small business etc – must also be accounted for. To subject all to the same would be disproportionate.
44 Corporate Liability	Guidelines under the bill should allow organizations to structure in a way that responsibility within is clearly indicated in terms of personnel in charge, so that accountability is conducted accordingly as well instead of arbitrary judgments on who should be made responsible, either by the organization or by the Authority.
46 Appeal	Section 46(1) states that an appeal is either to go to a High Court OR to a Tribunal to be established by the Federal Government. Any forum to hear appeals should be constituted through this bill so there is clarity and it comes into effect when the bill does. Left to the Federal Government, it may not even be established much after.

	Establishing the Tribunal and how it is to operate will also make clear when an order is to go into appeal there and when to the High Court, or confusion will prevail. The 30-day appeal window before the High Court should be qualified with a provision, subjecting it to the provision of all required documents and a certified copy of the order by the Authority.