The Dialogue™
INFORM ENGAGE IDEATE

APRIL 2022

RESEARCH PAPER

Building Effective and Harmonised Data Protection Authority

Strategies for Structural Design and Implementation

Kamesh Shekar[1]
Senior Research Associate

Author works with The Dialogue, India as Senior Research Associate and he is a Fellow at Internet Society.
Email ID: kamesh@thedialogue.co. Author would like to thank Manreet Khara for her research assistance.

Author: Kamesh Shekar

His area of research covers informational privacy, surveillance technology, intermediary liability, safe harbour, issue of mis/disinformation on social media, AI governance etc.

Edited By : Kriti Singh

Designed By : Diksha Kumari

Executive Summary

As India is stepping up its digitalisation efforts, technology is making its impression in various sectors. While technology has a positive side of the story where it thrust the society to better service, welfare delivery methods, crisis management and connectivity, it has also created gaps in the regulatory perimeter. To bridge these identified gaps in the current system, policymakers have moved towards framing new regulations/rules that apply to the same entity performing multiple functions or the same function but different regulations in a disjointed and ad-hoc manner. This multiplicity in regulations/rules can cause various problems at the receiving end, like confusion, repetition, over-regulation, compliance burden etc. Besides, vague interpretation of these provisions also risk sub-optimal approaches to standard-setting, and regulatory arbitrage and rely on discretion rather than a uniform application of the law. Therefore, we believe the future Data Protection Authority (DPA), envisioned under the Personal Data Protection Bill 2019 (JPC has suggested new version titled Data Protection Bill, 2021), must be done through greater regulator synergy, and responsive policymaking.

To effectuate this, in the paper, we map the possible clashing scopes and provisions prone to multiple interpretations within various data regulations in India. By doing this, we identify emerging challenges towards harmonising digital laws in India and suggest means and strategies that would aid the future DPA in building synergy.

In section 2, the paper discusses the status quo of the data protection landscape and various data sharing frameworks of India. This section shows the disjointed manner under which the policies and frameworks are developed using different routes such as legislation, subordinate rules by the executive, and delegated regulation through sectoral regulators and ministries. Some of the key legislation and data sharing frameworks discussed in this section are (a) Information Technology (Amendment) Act, 2008 (b) Competition Act, 2002 (c) Consumer Protection (E-Commerce) Rules, 2020 (d) Draft Non-Personal Data Governance Framework (e) Guidelines for democratising the existing geospatial data and maps (f) NITI Aayog's Data Empowerment & Protection Architecture (DEPA) (g) National Digital Health Mission: Health Data Management Policy (h) The India Digital Ecosystem of Agriculture (IDEA) (i) India Data Accessibility and Use Policy.

Analysing various conflicting and overlapping scopes in section 2, the paper suggests the first step toward harmonisation as weeding out the overlapping and conflicting scopes and bringing them to congruence with a single framework of data protection while enforced in a coordinated way. The paper proposes a phased smoothening process following the principles suggested in this paper, involving regulators and policymakers, who overlap within the perimeters of DPA. On completion of the smoothening process, to have coordinated and uniform enforcement of the data protection framework, the paper proposes setting up a data protection board. The board will act as a high-level coordination body comprising regulators (including DPA), policymakers (both executive and legislator) and the judiciary.

In section 3, the paper moves toward the rule-making process, one of the key functions of the DPA. Analysing the current state of rule-making, which is both ad-hoc and lacks technical expertise, the paper suggests some strategies for moving towards responsible regulation. We suggest a three-pronged approach - create a sandbox mechanism to understand innovations, conduct a prevalence-based complaint audit to understand the gaps and enact a separate administrative law to hold regulators and policymakers accountable to a principled-based approach.

Finally, in section 4, the paper analyses the issues with the existing grievance redressal system and suggests methods to enhance the capacity. The paper highlights two significant problems with the existing grievance management system as (a) lack of coordination horizontally (in terms of various coexisting systems and mandates) and (b) lack of agility in terms of resolution. To weed out this concern, the paper suggests a calibrated hierarchical grievance redressal mechanism with horizontal and vertical coordination (between different elements of the system) and agility proofing. The proposed calibrated grievance redressal mechanism must involve IVR, ODR systems, etc., and traditional systems like appellate tribunal and entities grievance management systems.

As India moves over the needle on digitalisation efforts, this paper emphasises that regulation and grievance management systems must be coordinated, updated, and efficiently used by operationalising the strategies and recommendations suggested in this paper.

TABLE OF CONTENTS

1. INTRODUCTION

India is witnessing tremendous growth in digitalisation efforts, where technology is making its footprint in various sectors. While technology positively impacts society by enabling innovation in business models, providing better service/welfare delivery methods, and helping in crisis management and connectivity, it has also created gaps in the regulatory perimeter. In deciding what interventions would best solve the identified gaps in the current system, policymakers have started framing many new regulations/rules.

In December 2019, the Personal Data Protection Bill 2019 (PDP Bill) was introduced in the Indian parliament by the Minister of Electronics and Information Technology. It was then referred to the Joint Parliamentary Committee (JPC) for fine-tuning through consultation with various stakeholders. The objective and reason for enacting this bill dates to August 24, 2017, when the Supreme Court of India delivered its judgement on Justice K.S Puttaswamy and others vs Union of India, declaring privacy as a fundamental right under Article 21 of the Indian Constitution. The judgement also directed the Government of India to bring in a robust data protection regime for the country.

It has been about two years since the PDP Bill was referred to the JPC; meanwhile, various data regulations and governance frameworks at different capacities have been floated in India in a disjointed ad-hoc manner. The JPC, after two years of deliberation over the PDP bill, tabled its report and draft Data Protection Bill, 2021 in the 2021 winter session of the parliament. While the committee had provided some significant suggestions to the PDP Bill, concerns related to the harmonisation of various data regulations and coordination of various ministries and sectoral regulators still remain unaddressed.

This multiplicity in regulations and rules without synergy would cause various problems at the receiving end, like confusion, repetition, over-regulation, compliance burden etc. Besides, vague interpretations of the provisions under these also risk sub-optimal approaches to standard-setting, regulatory arbitrage and rely on discretion rather than a uniform application of the law.

As the PDP Bill (JPC has suggested new version titled Data Protection Bill, 2021) provides a contour to set up a Data Protection Authority (DPA) that will protect the interest of data principle, formulate rules, functions, penalties and boundaries for data fiduciary and processor, supervise compliance to the bill (Act once enacted), and perform an adjudicatory role in matters of privacy. We believe this future regulator must be done through greater regulatory synergy, and responsive policymaking. To effectuate this, in this paper, we map the possible clashing scopes and provisions prone to multiple interpretations within various data regulations in India. By doing this, we identify emerging challenges towards harmonising digital laws in India and suggest means and strategies that would aid the future DPA in building synergy.

Identifying three major matters of contention, the following sections of the paper are sketched as follows. In section 2, we discuss the regulatory conflict issue by mapping various clashing scopes and provisions prone to multiple interpretations within data regulations in India and suggest mitigation strategies for the same. In section 3, we discuss the problem of ad-hoc rule-making and suggest ways to move towards responsible rule-making. Finally, in section 4, identifying multiple grievance management systems in place of one, we propose a calibrated grievance management system.

2.LEGION OF DIGITAL LAWS IN INDIA

Currently, in India, regulations pertaining to technology are being made in a disjointed manner under different routes such as legislation, subordinate rules by the executive, delegated regulation through sectoral regulators and ministries. This multiplicity of regulations and rules causes various supply-side, demand-side (discussed in section 4) and regulatory issues.

The foremost supply-side issue emerging out of a multiplicity of regulations is compliance uncertainty and the feeling of over-regulation, which goes against the expansionary policy sentiment and contributes to investment barriers. Besides, applying different regulations to the same entity performing multiple functions would increase the compliance cost for them, which in the case of start-ups, could cause an entry barrier. Moreover, multiplicity of laws can cause regulatory arbitrage. The entity might find a way to comply only with the most favourable (per its business) regulation at the cost of escaping other crucial mandates under other regulations. In addition to this, a lack of uniformity in consumer or entity's understanding would lead to contradictory interpretations in case of a dispute.

Therefore, to have a holistic picture of data protection, we compare data regulations in India to map conflicting scope and provisions and provide measures to bring in synergy.

2.1. CONFLICTING AND OVERLAPPING SCOPE

2.1.1. LEGISLATION

(a) Information Technology (Amendment) Act, 2008[2]

There are various provisions under Information Technology (Amendment) Act, 2008 (IT Act) that mandate data protection and privacy, such as Section 43[3], 43A[4], 72A[5], and 66E[6]. While Section 43A of the IT Act will be omitted with the enactment of the PDP Bill , other data protection and privacy-related provisions under the IT Act will remain, which may lead to confusion and regulatory arbitrage. Because, currently, entities who fall under the definition of 'intermediary' come under the purview of the IT Act, but with enactment of the PDP Bill, 'intermediary' will also turn into data fiduciaries (in most cases) who will be mandated to follow a different set of standards. While not all the data fiduciaries will be intermediaries, it is important to ensure that wherever there is overlap it must be smoothened.

Besides, in February 2021, the central government notified Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021). Part II of the IT Rules 2021 sets out the due diligence and grievance redressal mandates for the intermediary, social media intermediary and significant social media intermediary. The IT Rules 2021[8] stands against some of the features of the PDP Bill i.e. data

[2]As per section 87 of the IT Act, 2000, the central government of India can make rules (delegated legislation) under the IT Act, 2000, such as recent IT Rules 2021

[3]Penalty and compensation for damage to computer, computer system, etc.

[4]Compensation for failure to protect data

[5]Punishment for disclosure of information, knowingly and intentionally

[6]Punishment for violation of privacy

[7]The government had initiated a preliminary conversation on amending the IT Act, especially section 43-46, to introduce new penalties for social media companies and individuals while criminal provisions as part of the law (Bhardwaj, 2021)

[8]One of the most debated aspects of the IT Rules, 2021 pertaining to part II is Rule 4(2), which mandates significant social media intermediaries to identify the first originator of a particular message. While there can be various ways to trace the first originator, in practicality, most of the means break the end-to-end encryption (Grover, Rajwade, & Katira, 2021). Breaking end-to-end encryption gives backdoor entry to every conversation of the consumers (directly or in-kind) to the government (on request), the private entities, and others such as hackers etc.

retention (Clause 9), right to be forgotten (Clause 20), privacy by design (Clause 22). In addition, the rules[9] don't pass the proportionality doctrine test[10], which was emphasised in the Puttaswamy judgement (Rizvi & Singh, 2021). Some of the provisions in IT Rules 2021 also violate few universal human rights and values, such as freedom of expression [which is briefly touched upon in the PDP Bill [Clause 3(20)(ix)].[11]

Therefore, as we move towards harmonisation, DPA has to move away from the zero-sum framework and find a striking balance between privacy and security.

(b) Competition Act, 2002

The responsibility of the Competition Commission of India (CCI/Commission) (enforcing the Competition Act, 2002) is to prevent practices with adverse effects on competition and sustain healthy competition in the market. With the emergence of digital markets, the application of the Competition Act has become convoluted. In a report published by CCI on the telecom sector (Market Study On The Telecom Sector In India, 2021) in January 2021, the Commission analysed the synergy between competition and privacy in a non-price competition market. The report notes that abuse of dominance can be in the form of lower privacy protection for consumers, as sub-optimal privacy standards can impact consumer welfare.[12]

Besides, the report (Market Study On The Telecom Sector In India, 2021), in line with other scholars (Khan, 2017), notes that lower data protection can also cause exclusionary behaviour, which falls within the ambit of the Competition Act, 2002. In addition to this, recognising that nothing is free in the platform economy as we pay in the form of our personal and mixed data (which platforms monetise indirectly), the competition law review committee (Report Of Competition Law Review Committee, 2019) examined the definition of 'price' under section 2(o) of Competition Act. The committee concluded that the definition is broad enough to recognise non-monetary aspects like 'data' under section 2(o).

While the CCI is looking into competition aspects of privacy and data protection from the consumer welfare standard, DPA needs to harmonise this aspect within its definition of harm [Clause 3(20)] and data protection impact assessment (Clause 27) function to have a holistic picture of data protection. Besides, in the report on the telecom sector (Market Study On The Telecom Sector In India, 2021), CCI has acknowledged that there is a need for better regulatory design and improved lines of communication between DPA (other regulators as well) and CCI to harmonise the decisions to ensure robustness and consistency.

(c) Consumer Protection (E-Commerce) Rules, 2020

The Department for Promotion of Industry and Internal Trade in June 2021 proposed amendments to the Consumer Protection (E-Commerce) Rules, 2020, to lay out regulatory frameworks for E-commerce in terms of consumer protection and fair competition. Previously the government released versions of the Draft E-commerce Policy in 2019 and mid-2020, which didn't make it through the cut. But the rules are on a path of abjuring as well because (a) no unanimity amongst the ministries. For instance, the finance ministry voiced its concern about the excessive nature of the rules, which would hamper tax revenue and ease of doing business (Sharma, 2021). (b) These rules might increase compliance costs for the start-up. Besides, the clauses in the rules fetched their hand into Competition Act 2002 and missed out on aspects related to personal and non-personal data protection which is crucial in the non-price market like E-commerce (where we also pay in the form of data in addition to purchases (Tripathi & V, 2021). Therefore, until we have a holistic regulatory framework for the E-commerce and digital economy, DPA must fill in the gaps. In future,

---

[9]The order for tracing under the IT Rules 2021 shall only be passed for safeguarding sovereignty and integrity of India, the security of the State, friendly relations with foreign states, or public order, or incitement to an offence

[10]The extent of state interference on rights needs to be proportional to the goal it seeks to achieve through it. This doctrine was famously used in a landmark judgement in the realm of privacy happened when the Supreme court struck down provisions of the Aadhaar Act under lack of purpose limitation

[11]Under Clause 3(23)(ix) of JPC version of Data Protection Bill, 2021

[12]In concurrent with this outlook, the Competition Commission of India filed a suo moto case against WhatsApp concerning its update in terms and conditions and privacy policy (Suo Moto Case No. 01 of 2021)

any frameworks related to E-commerce have to be developed in collaboration with DPA to have uniformity in data regulations.

2.1.2. DATA SHARING & TRANSFER FRAMEWORK AND POLICY

Globally, the countries are in the process of extending their data protection frameworks to find a proper balance between privacy and extracting utility from data (Matthan, 2021). While the scope of the PDP bill is to protect informational privacy and create a framework for organisational and technical measures in data processing, the DPA needs to keep up with the current pace of regulatory developments in the country, which is pushing the needle towards enabling data transfer and sharing arrangements.

(a) Draft Non-Personal Data Governance Framework

The expert committee on Non-Personal Data (NPD) governance floated the revised version of the report in December 2020. In the report, the committee proposes to set up a national-level regulation that will (i) vest rights over non-personal data, (ii) enable data sharing to unlock the economic benefits from NPD, (iii) address privacy, re-identification of anonymised personal data, and prevent misuse of and harms from data. Outlining various actors as part of this regulation, the committee proposed a new kind of business classification called 'Data Business' (both data custodian and data processor), which collects and manages personal data and NPD. This new classification will create uncertainty and confusion as the data business would be classified as data fiduciary and data processor under the PDP Bill. This move also highlights that the same entity must comply with two different regulations for different functions (i.e. functions related to personal data and NPD). In addition, as data trustees will also be considered as data custodians, it is unclear if they will be classified as data fiduciary under the PDP Bill (in terms of re-identification). Besides, the committee also suggests that the data business has to register in India beyond a threshold, which is similar to Clause 26(2) of the PDP Bill pertaining to significant data fiduciary.

While the committee does acknowledge that the threshold of data business must be harmonised with that of significant data fiduciary, there is no clarity on whether an entity has to register under both DPA and as specified under NPD regulation. This could cause regulatory arbitrage (if the regulators are not harmonised) and increase the compliance cost. On the other hand, the concept of network effect (which entities use in their favour), which is actively discussed by CCI (Market Study On The Telecom Sector In India, 2021), has implications on collective privacy, which the committee discusses in terms of NPD.

Therefore, while the committee does acknowledge and opens the scope for harmonisation between the proposed Non-Personal Data Protection Authority (NDPA) and DPA (and other regulators like CCI), it is important to smoothen the overlaps (like mentioned above) and sketch a regulatory design that will bring these regulators to work in tandem.

The JPC recommended including provisions on NPD as part of the PDP Bill, making it into Data Protection Bill, 2021. However, this paper suggests that it is ideal for the PDP Bill to refrain from having provisions on Non-Personal Data to avoid the overlap in regulatory boundaries. At the same time, smoothening the overlaps in regulatory boundaries is discussed in the Section 2.2.

[13]With emergence of Data Protection Bill, 2021, the objective and scope of PDP Bill, 2019 has become nebulous
[14]The report defines NPD as anything which is not personal data and anonymised data which doesn't follow under the ambit of PDP bill
[15]Refer section 6 of Report by the Committee of Experts on Non-Personal Data Governance Framework
[16]Refer point 7.7 of Report by the Committee of Experts on Non-Personal Data Governance Framework
[17]Unclear on under whom does the data business register
[18]Point 5.3(ii): Harmonisation in terms of setting the borders of DPA and NDPA
Point 6.3(iii): Harmonisation in coming up with data-related directories and disclosures
Point 7.10: Harmonisation in the creation of NDPA
Point 7.12 (ii, iii): Harmonisation in task and focus of NDPA

(b) Guidelines for democratising the existing geospatial data and maps

The government of India (GOI), on February 15, 2021, liberalised the mapping industry and democratised the existing geospatial datasets for enhancing domestic innovation and economy. Geospatial data refers to geographic information on natural or human-made, physical or imaginary features, including below or above the Earth's surface. As the definition of geospatial data stands, it would categorise (i) under the proposed NPD regulation as a subset of non-personal data over which the community has a right and pose collective privacy issues (ii) under the PDP Bill (as mixed data which also brings out competition implications such as exclusion from services (Khan, 2017) (Report Of Competition Law Review Committee, 2019). This highlights that the same function performed by an entity is subjected to condescending regulations, resulting in confusion.

In the guidelines[19], the GOI has allowed any Indian entity[20] to collect, generate, prepare, disseminate, store, publish, update and/or digitise geospatial data and maps within the territory of India with notified negative list of sensitive attributes[21] that would require regulation before anybody acquires and attribute. A Geospatial Data Promotion and Development Committee (GDPDC) will be formed by the Department of Science and Technology (DST) to weed out issues arising out of negative attributes lists and the regulations proposed on those attributes. While democratising the existing geospatial datasets would help enhance economic activities of various sectors such as e-Commerce, agriculture, cab aggregator services etc., it is crucial to harmonise these guidelines as well the functions of GDPDC within the scope of DPA (which would work in synergy with other regulators) to ensure data protection and privacy.

(c) NITI Aayog's Data Empowerment & Protection Architecture (DEPA)

Adding to the final layer of India Stack[23], the Niti Aayog's recent draft DEPA policy[24] proposes a "new class of business" titled consent manager. The consent manager will act as a conduit between (i) data principle, (ii) data fiduciaries who hold the data and (iii) data fiduciaries whom the data principle seeks to transfer the data.

Following the draft DEPA policy, the Indian central bank operationalised its consent manager framework called Account Aggregator. Licensed under the category of NBFC, Account Aggregator (NBFC-AA) will collect and share consumers' financial information with their consent from a financial information provider[25] to a financial information user.[26] As NBFC-AA would act as a consent manager for financial information transfer, they would fall within the ambit of DPA [Clause 23(5)] as they have to register under the authority. This highlights the overlapping scope, which would result in regulatory arbitrage and confusion. The technical aspects prescribed by RBI for NBFC-AA (NBFC - Account Aggregator (AA) API Specification, 2019) is mostly congregant with privacy by design principle (Raghavan & Singh, 2020b), but the privacy protection at the ends, i.e. FIU and FIP, falls within the ambit of DPA as the financial information is defined as sensitive personal data.

While RBI has sorted out an exemption from the PDP bill and doesn't want financial information to be categorised under sensitive personal data (HT, 2020), the DPA needs to work in tandem with RBI and other financial sector regulators to have a holistic approach towards data protection and to have uniformity in the regulation. Besides, as more new businesses could emerge following DEPA, it is important to harmonise DEPA within the scope of DPA.

---

[19]Notified by the Department of Science and Technology (DST)
[20]Any Indian citizens, government entities, Indian companies, etc
[21]https://dst.gov.in/sites/default/files/Final%20List%20of%20Negative%20Attributes.pdf
[22]Negative attribute lists is subjected to revisions
[23]India stack is India's digital financial infrastructure which has three layers: (i) Identity layer (Aadhaar, eKYC, eSign etc.), (ii) Payment layer (UPI, AePS etc.), (iii) Data empowerment (Account aggregator, consent artefact etc.) (NITI Aayog)
[24]This draft policy was put together by financial sector regulators (RBI, SEBI, IRDAI and PFRDA) and the ministry of finance
[25]Refer Section 3(xi) in Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016
[26]Refer Section 3(xii) in Master Direction- Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016

(d) National Digital Health Mission: Health Data Management Policy

As envisioned under the National Health Policy, 2017, the Ministry of Health and Family Welfare set up the National Digital Health Mission (NDHM) - a federated structure. As per one of the guiding principles (i.e. Security and Privacy by Design) of NDHM, the Health Data Management Policy was floated. In this policy, NDHM outlined the process of issuing a health ID to data principal and procedures for enabling health information transfer between health information provider[28] to health information user[29] through the NDHM network, amongst other arrangements within the National Digital Health Ecosystem (NDHE). As health information is one of the sub-set of sensitive personal data under the PDP Bill , all the players within the NDHE, including NDHM (as it provides the network for data transfer), will come under the ambit of DPA.

The policy proposes to set up NDHM Data Protection Officer (NDHM-DPO) to ensure adherence by the players within the NDHE, but it has been noted that the absence of penalty in case of breach leads to non-compliance with the policy (Mariwala & Kwatra, 2021). Therefore, to avoid regulatory arbitrage and have better enforcement of data protection and privacy measures, Health Data Management Policy must be advised by the DPA who is already vested with the obligation to make rules for health information as part of its broader mandate.

(e) The India Digital Ecosystem of Agriculture (IDEA)

The Department of Agriculture, Cooperation and Farmers Welfare recently signed a Memorandum of Understanding (MoU) with Microsoft Corporation, Star Agribazaar, Patanjali Organic Research Institute for agricultural management and services, Amazon Internet Services, and Esri India for setting up AgriStack. Like IndiaStack, AgriStack also has technological layers with players across central and state governments within a federated system. The framework of 'AgriStack' envisioned (i.e., a unified platform for collecting technology and databases focused on the agricultural sector) in the consultation paper titled The India Digital Ecosystem of Agriculture (IDEA) has some privacy concerns (Kapil, 2021).

While farmers' personal information is a subset of personal data, being cognisant of these new developments (potential future developments along the same lines), DPA must ensure to tie these loose ends to close the gaps in data protection regulation.

(f) India Data Accessibility and Use Policy

Recently MeitY had also floated the draft India Data Accessibility and Use Policy. The policy envisions setting up the India Data Council which comprises Data Officers and Chief Data Officers of Departments of Government of India and State Governments. The role of the India Data Council is not limited to defining frameworks for important Datasets, but also includes finalising Data standards and Metadata standards as well as reviewing the implementation of the policy. As standard-setting would be one of the roles of the Data Protection Authority, the council has an overlapping scope.[30] The council must work closely with the Data Protection Authority (as provisions on non-personal data are expanded in Data Protection Bill 2021) and evolve its policies and SOPs in congruence with the regulations surrounding data. Also, working in tandem with Non-personal Data Protection Authority (If constituted) is crucial. Besides, the India Data Council should work in synergy with other sectoral regulators as well.

[27]The government launched NDHM at the national level as Ayushman Bharat Digital Mission.
[28]Refer to section 4(s) in Health Data Management Policy
[29]Refer to section 4(t) in Health Data Management Policy
[30]Union minister of state for electronics and IT said any overlap of the policy with the Personal Data Protection Bill will be addressed (Agarwal, 2022).

2.2. MITIGATIONS

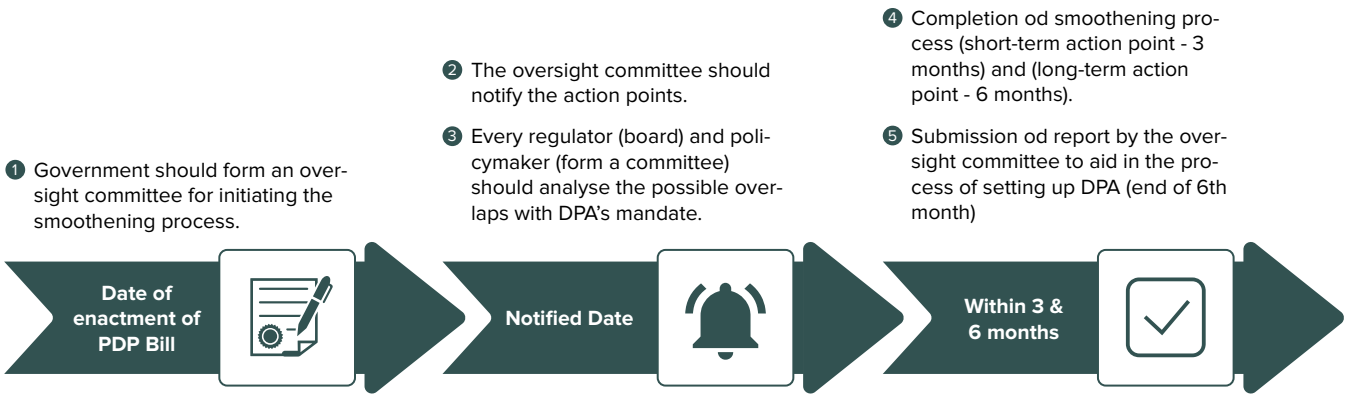
Analysing various conflicting and overlapping scopes in the previous section, two things that stood out are the lack of uniformity and coordination amongst the various regulations and regulators, respectively. This section will look into how we can mitigate the same to have India's harmonised data protection framework.

2.2.1. BRINGING ABOUT UNIFORMITY

As the first step toward harmonisation, it is essential to weed out the overlapping and conflicting scopes and bring them to congruence with a single framework of data protection while enforced in a coordinated way. A similar set of strategies was proposed in the Report of the Financial Sector Legislative Reforms Commission (FSLRC)[31] to consolidate some of the provisions in financial regulation. While this proposal was not picked up, it is essential to note that the FSLRC recommendation on consolidation of regulatory architecture was for the existing regulator. In contrast, DPA is a new fourth branch regulator [32] yet to be established. Besides, only a particular aspect (i.e. provision related to data protection) of the existing regulations must be consolidated with the functions of DPA, not the other functions of related regulators/ policymakers per se.

Thus, zero-step towards making future DPA should involve regulators and policymakers, who overlap within the perimeters of DPA, in terms of building mechanisms for coordination and smoothing following the principles suggested in this paper (refer to section 3.2.3). Moving towards a uniform data protection framework would also require planning and coordination from the government and regulators to ensure a seamless process without creating regulatory uncertainty. To oversee this process, the government should form a committee with representation across the board, i.e. legislation and judiciary, who would, in turn, come up with overarching action points for each regulator and policymaker depending upon their territory. The committee should categorise the action points into short-term and long-term according to the nature of the amendment requirements. For instance, amending legislation would take more time than guidelines, rules etc. The below figure suggests a process against a timeline.

Figure 1: Blueprint for smoothening process



[31]The Ministry of Finance constituted FSLRC in March 2011 to review the legislation governing Indian financial systems and propose recommendations for redrawing the legislation.

[28]Some of the existing fourth branch regulators are ECI, NHRC etc.

2.2.2. FORMING A DATA PROTECTION BOARD

Completing the smoothening process brings us to the question of enforcing a uniform data protection framework for India. This would require high-level coordination amongst the regulators and policymakers. While there are provisions for coordination and harmonisation (refer to table 1) in some of the legislation and data sharing & transfer framework and policy, including the PDP bill, they stand disjointed and unclear (as discussed in section 2.1.2).

Table 1: Mapping provisions on harmonisation and coordination

Legislation/data sharing & transfer framework and policy	Provisions
PDP Bill	Clause 50 (2) & clause 56 – coordination amongst the functioning regulators and governments.
Competition Act, 2002	Section 21 and 21A – coordination between CCI and other statutory authority. Point 72 - The market study report on telecom by CCI emphasises that CCI has to work in tandem with the envisaged Data Protection Authority.
Draft Non-Personal Data Governance Framework	Chapter 5.3 – Harmonisation between NPD regulation and PDP Bill through amending provisions in PDP Bill.
National Digital Health Mission: Health Data Management Policy	Section 6 – MoHFW and MeitY is envisaged to provide overall guidance to the NDHM.

Therefore, similar to European Data Protection Board[33], the Indian government (in association with legislature and judiciary) needs to constitute a Data Protection Board (DPB). The EU's Data Protection Board model does fit our case because it was formed for harmonisation.[34]

DPB as an independent body must look into the consistent application of uniform data protection. This board should comprise regulators (including DPA), policymakers (both executive and legislator) and the judiciary. The DPB must promote cooperation amongst the regulators and policymakers and DPA, provide guidance and clarifications on the data protection framework, and give suggestions to various regulators and policymakers in cases related to data protection. in the form of advice.

Besides, the lack of technical expertise by DPA in understanding nuanced aspects of the technology sector (which would need sectoral expertise, be it antitrust or financial sector issues) can be solved through DPB as they have representation of all the regulators who have a stake in the data protection ecosystem. In addition to this, DPB should also form an external technical expert council (whenever necessary) to advise

[33]EDPB is an EU body in charge of the application of the General Data Protection Regulation (GDPR)

[34]While GDPR is regulation (the term regulation in EU refers to binding for the members countries to follow), still it provides flexibility for member countries to have their own data protection framework and authority

the board on matters which require technical knowledge support. The expert council should mandatorily engage with civil society members and other stakeholders through consultation as part of their deliberations. A similar kind of expert council system is currently implemented in Brazil (which has many similarities to India, in terms of multiplicity in digital laws) under their data protection regime, which has a similar story to India (Zanfir-Fortuna, 2020).

3. RULE-MAKING ISSUE

Moving toward the rule-making process, in this section, we analyse the current state of rule-making, which is both ad-hoc and lacks technical expertise and suggest some strategies to move towards responsible regulation.

3.1. AD-HOC RULE-MAKING

What are the instances?

The state of regulatory reflex in India regarding the technology sector is more ad-hoc and reactive than responsible. This ad-hoc nature illuminates from the lack of technical expertise and agility, which leads to multiple grounds of the regulation (refer to section 2.1) popping up in silos, not taking cognisance of others. Besides, the lack of technical expertise has also brought to fore various trouble in the sector, where the regulator might choose sub-optimal regulation in place of responsible one. For instance, the technology experts have been alarmed that IT Rules, 2021 is problematic because of its provision on the originator traceability [Part II Rule 4(2)] for significant social media intermediaries (messaging platforms). Though the government hasn't sought to break end-to-end encryption explicitly through this provision. Seeking a backdoor mechanism highlights a lack of technical expertise on the government front, because it is equally problematic (Robertson, 2021) and dilutes the encryption technology. In addition to this, we also see that policymakers tend to move towards the highest form of regulation when they don't understand technology, such as a ban[35] which is both disproportionate and less business-friendly.

Why is this happening?

One of the key critiques of the PDP Bill, 2019 (is that it is taking too long to take effect[36]), and such a delay may render it obsolete given the fast pace of technological advancement as the subject matter of the Bill may need changes and updates by the time it comes into effect. The Bill focuses on the responsibility of data fiduciaries, which are third-party intermediaries (under some other regulation, refer to section 2.1); however, with the rapidly changing landscape of technology, data fiduciaries (defined in the Bill) may not be the only data handlers, and instead, will be increasingly replaced by new technologies and players, which may not currently fall under the definition like data brokers. This exclusion allows new technology and players to violate data protection laws and manipulate consumer data as it sees fit. In order to remedy such exclusions, rule-making will have to keep pace with technological development, even though the technology is advancing at an exponential pace in geometric progression according to Moore's Law[37], while policymaking is barely scraping the trails of arithmetic progression.

Therefore, as we move towards harmonisation, DPA needs to keep up with the technology's pace and be responsible for its actions.

---

[35]Parliamentary standing committee on home affair suggested government to ban VPN (HT, 2021)

[36]It has been almost four years since the K.S. Puttaswamy-I judgment came and three years since the Srikrishna Committee came out.

[37]In 1965, George Moore posited that roughly every two years, the number of transistors on microchips will double. Commonly referred to as Moore's Law, this phenomenon suggests that computational progress will become significantly faster, smaller, and more efficient over time

3.2. MOVING TOWARDS RESPONSIBLE RULE-MAKING

How is it possible for policymaking to keep up with technology and be responsible for its actions? We suggest a three-pronged approach - create a sandbox mechanism to understand innovations, conduct a prevalence based complaint audit to understand the gaps and enact a separative administrative law to hold regulators and policymakers accountable to a principled-based approach.

3.2.1. SANDBOX MECHANISM TO UNDERSTAND INNOVATIONS

Indian legislators and regulators often brush off newer technologies that they don't understand yet for fear of insidious intent and hidden features they may miss, as is evident from the RBI's then disdain and suspicion of cryptocurrency. Fear dissipates by making innovations less alien by understanding them. Policymakers and regulators are overwhelmed by the pace of technological advancement, therefore to aid them, we propose a sandbox mechanism where the entities can test their innovation against the set principles notified by the regulator taking cognisance of other interests of other regulators.[38] We believe the sandbox mechanism can aid regulators to keep up with the technology by assessing their compatibility and violations to check whether they are compliant with the principles set out.

Moreover, the sandbox mechanism effectively introduces new technology to lawmakers and regulators to prevent a fear-based reactionary ban and instead seek exemptions for new technology rather than ad hoc legislation. While technology can be dynamic, changing legislation can be a time-consuming and strenuous process so we suggest giving exemptions based on principles. Therefore, we believe that a sandbox would bring in an accommodative stand towards a new technology as long as it ticks all the principles.

While PDP Bill, 2019[39] envisions a sandbox mechanism, central, state governments and regulatory bodies in India already use the sandbox mechanism for testing innovations. For instance, the RBI introduced the Regulatory Sandbox in 2019. This sandbox aims to bring innovation to financial services by allowing businesses to live test their solutions in a controlled regulatory environment.[40] Since 2019, RBI has hosted four regulatory sandbox cohorts on retail payments[41] (six entities successfully exited), cross border payments [42], MSME lending[43] and prevention and mitigation of financial fraud.[44] At the state level, one such initiative is the establishment of the Karnataka Innovation Authority and the mechanisation of the sandbox mechanism under it.[45] The authority through this has enabled start-ups and businesses to test their innovations without legal barriers. The sandbox aims to bring innovative businesses and emerging technologies under legal perimeter through testing until the existing legal framework evolves to the pace of technological development.

---

[38]This can also aid in cross border data sharing arrangements like Adequacy Decision

[39]The Clause 40 PDP Bill (JPC has suggested new version titled Data Protection Bill, 2021) provides for a sandbox mechanism where new technology can be tested by the innovators under the scrutiny of the regulator

[40]Enabling Framework for Regulatory Sandbox. (2019, August 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/PublicationReportDetails.aspx?UrlPage=&ID=938time

[41]Regulatory Sandbox (RS): First Cohort on 'Retail Payments' – Exit. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52217

[42]Regulatory Sandbox (RS): Second Cohort on Cross Border Payments – Test Phase. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=52218

[43]Reserve Bank Announces Opening of Third Cohort under the Regulatory Sandbox. (2021, September 13). Reserve Bank of India. Retrieved January 21, 2022, from https://www.rbi.org.in/scripts/FS_PressRelease.aspx?prid=52219&fn=9

[44]RBIs fourth regulatory sandbox cohort is on prevention of financial frauds. (2021, October 9). Business Standard. Retrieved January 21, 2022, from https://www.business-standard.com/article/finance/rbi-s-fourth-regulatory-sandbox-cohort-is-on-prevention-of-financial-frauds-121100900048_1.html

[45]Joshi, B. (2020, February 24). Karnataka government eyes innovation push through Innovation Authority Bill. Deccan Herald. Retrieved April 11, 2022, from https://www.deccanherald.com/state/top-karnataka-stories/karnataka-government-eyes-innovation-push-through-innovation-authority-bill-807509.html

As some of these technological innovations fall within the regulatory perimeter of sectoral regulations, state policies and the PDP Bill, it is important to harmonise the sandbox mechanisms. A concerted effort is needed from the regulators and governments such that innovations are tested for both sectoral regulation, state policies and data protection compliances through having a single integrated sandbox mechanism.

3.2.2. PREVALENCE BASED COMPLAINT AUDIT TO UNDERSTAND THE GAPS

A feedback mechanism based on analysing the prevalence of complaints[46] received by the DPA, DPB, and calibrated grievance management system (refer to section 4.2) is one way of identifying gaps in current regulation. For instance, Facebook reinstated the award-winning image of a naked girl fleeing napalm bombs during the Vietnam War after receiving negative feedback following its takedown. While Facebook received this feedback through newspapers and civic movements, this event still shows that aggregating grievances can provide feedback on policies and actions (Shekar, 2021).

If all the complaints received by regulatory bodies were to be analysed for prevalence, patterns would emerge to reflect where the mechanism has formed a void or lacks seamlessness. These complaints could flag the proportion of problems in different laws for pre-existing technologies and function as a signal of any new technological trends that aren't covered by regulation yet. Once this audit of complaints is conducted and data patterns emerge, the problem areas become more apparent and easier to solve. Newer technologies can then be studied, understood, and regulated, recurring problems can be addressed with alternative solutions, and any blockages in redressal mechanisms can be eased.

3.2.3. MAKING A CASE FOR ADMINISTRATIVE LAW & PRINCIPLE-BASED APPROACH

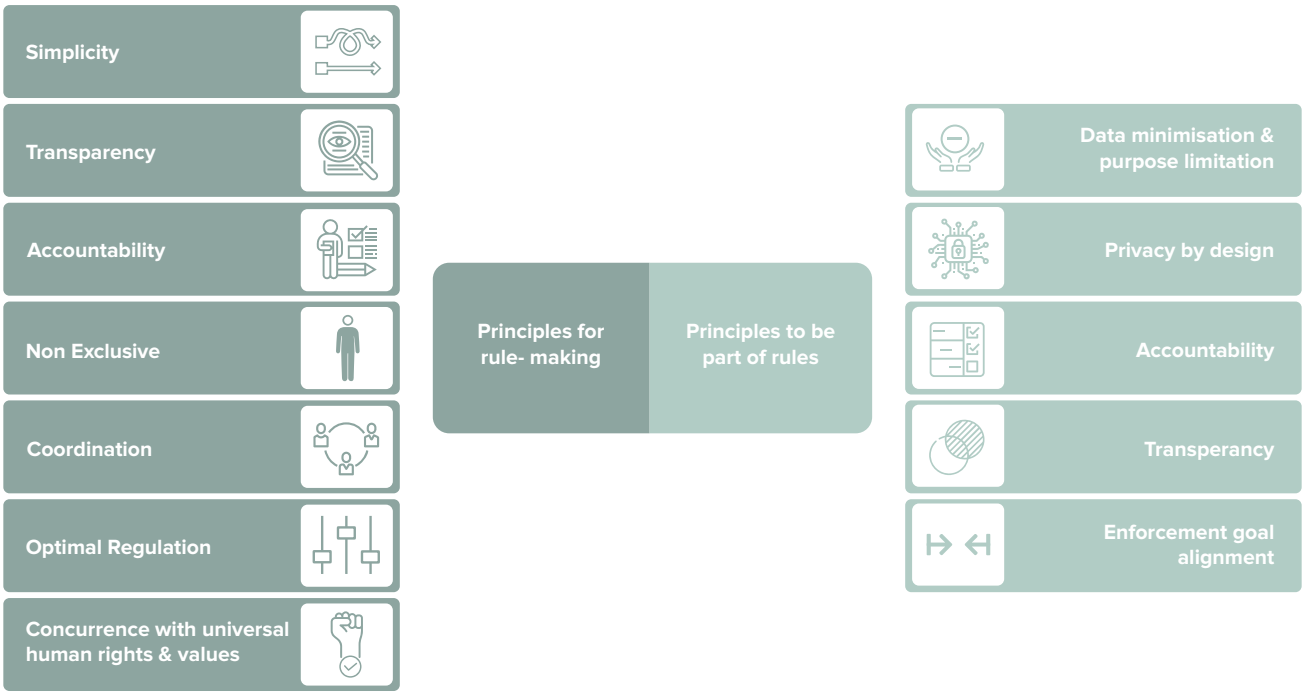
(a) Principle-based approach

Some key principles with respect to technology and data protection need to be identified and recognised as important. These principles must be held and promoted by DPB (refer to section 2.2.2) to preserve the country's uniform data protection framework. The principles outlined in this paper have been identified specifically for the Indian context and partially reflect the principles outlined in the GDPR.[47] We bucket them into two sets - (i) universal principles for the regulators to follow while making laws and (ii) principles related to the technology sector, which should be part of the rules (figure 2). These principles[48] have to be enforced by administrative law (as discussed below).

[33]EDPB is an EU body in charge of the application of the General Data Protection Regulation (GDPR)

[34]While GDPR is regulation (the term regulation in EU refers to binding for the members countries to follow), still it provides flexibility for member countries to have their own data protection framework and authority

Figure 2: Bucket of principles



Principles for rule-making

(i) Simplicity - To make the laws accessible to the layman and enhance the ease of conducting business by making them simple to understand.

(ii) Transparency - The process of rule-making has to be transparent, and prevalence based audit reports (refer to section 3.2.2) should be made public.

(iii) Accountability - The rule-making process has to be made accountable to external oversight such that the process is followed diligently.[49]

(iv) Non-exclusion - This principle should guide the rule-making process such that rules don't create any exclusion as one of the unintended consequences.

(v) Coordination - Amongst government, regulatory bodies and policymakers, and betweenthe different laws governing technology.

(vi) Optimal regulation - The regulation has to be proportional following purpose limitation and calibrated optimally to the nature of the issue to be tackled.

(vii) Concurrence with universal human rights & values - This principle should guide the rulemaking process such that the provision of the rules doesn't violate universal human rights and values like privacy, freedom of expression etc.

Principles to be part of rules

((i) Data minimisation & Purpose limitation - The data processed should not exceed the purpose for which it was collected and should not be held/stored post the completion of the purpose.

[49]Administrative law can also act as an accountability mechanism

(ii) Privacy by design[50] **-** The data infrastructure and processing mechanism should be privacy-friendly and don't trade-off privacy at the cost of business efficiency.

(iii) Accountability - The rules must prescribe a robust accountability framework involving actors like accessors and framers (Moss, Watkins, Singh, Elish, & Metcalf, 2021). The rules must follow stimulative policy measures, such that market mechanisms can be used for accountability. For instance, making a market for algorithmic rating systems could push the platforms towards performing better on the user outcome aspect.

(iv) Transparency - The information on the processing mechanism of the data must be simple and available. The data protection impact assessment and other audits reports must be made public.

(v) Enforcement goal alignment - The corrective actions provisioned in the rules must align with the enforcement goal which could be compensating for the harm, a moratorium for deterrence etc. The harms to be recognised should be both tangible harms like financial harms and intangible like emotional and psychological harms[51], reputational harms etc. Moreover, the causation of harm should not be the only factor for individuals to raise a complaint with the authority (Citron & Solove, 2022), where privacy concerns would have ex-ante i.e. before the harm is caused and speculative i.e., concerns could arise in long term.

(b) The framing of an administrative law

Currently, India doesn't have an overarching administrative law like what we have in the US (US Administrative Procedure Act, 1946 - refer to box 1) and in some form in the UK (UK FSMA 2000 - refer to box 1). Therefore, we suggest enacting an overarching administrative law for India. This law would provide overarching accountability and oversight, which streamlines procedures for the policymakers. This will also make the mechanisms and strategies suggested in this paper robust by moving toward a responsible rule-making process. The aforementioned principles need to be encoded in an administrative law so that they are binding upon any policymakers and regulators to be followed while making laws and incorporated as part of the law. Administrative law is imperative to hold regulators and policymakers accountable to a principled-based approach.

Box 1 - Learning from other jurisdictions

The US Administrative Procedure Act, 1946

The US Administrative Procedure Act, 1946 binds the US SEC and mandates a system of notice and comment while proposing legislation under S.553 wherein a general notice of proposed rule-making shall be published in the Federal Register. The notice shall include -

1. a statement of the time, place, and nature of public rule-making proceedings;
2. reference to the legal authority under which the rule is proposed; and
3. either the terms or substance of the proposed rule or a description of the subjects and issues involved.

The UK FSMA 2000

The UK FSMA 2000, lays down in detail the processes that the UK's Financial Conduct Authority (FCA) has to carry out before enforcing regulations.

S.155 of the UK FSMA 2000 states that if the Authority proposes to make any rules, it must publish a draft of the proposed rules in the way appearing to it to be best calculated to bring them to the attention of the public. That draft must be accompanied by

[50]Privacy by design has seven foundational principles - https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf
[51]JPC report and version of the data protection bill incorporated psychological harm as privacy concern.

1. a cost-benefit analysis;
2. an explanation of the purpose of the proposed rules;
3. an explanation of the Authority's reasons for believing that making the proposed rules is compatible with its general duties; and
4. notice that representations about the proposals may be made to the Authority within a specified time.

4. DISPUTE MANAGEMENT ISSUE

Having a robust grievance redressal mechanism to serve both entities and consumers is crucial. This section analyses the issues with the existing grievance redressal system and suggests methods to enhance the capacity.

4.1. MULTIPLE GRIEVANCE MANAGEMENT IN PLACE OF ONE

Currently, there are multiple forms of grievance redressal portals for entities and consumers to lodge their complaints with the regulator/policymakers. For instance, each financial sector regulator has its own ombuds, there is Cyber Appellate Tribunal under IT Act[52], PDP Bill envisages setting up an appellate tribunal etc. As grievance in the technology sector would tick the box of multiple tribunals and ombuds, the current disjointed way of operating grievance management might become obsolete, confusing, and onerous. This would also cause regulatory uncertainty[53], where the regulator/policymaker might deny redressal to a particular grievance stating this doesn't fall within their ambit. In addition, most legislations and data sharing & transfer frameworks and policies outline different grievance management systems for entities (refer to table 2), creating overlaps and confusion for the consumers.

Table 2: Multiplicity in grievance redressal mechanism

Legislation/data sharing & transfer framework and policy	Provisions	Mandate	Point of contact for consumers[54]	Time duration for resolution
PDP Bill	Clause 32	Data fiduciary to have effective grievance mechanisms toredress data principals complaints efficiently in a speedy manner	Data protection officer (in the case of significant data fiduciary) Any designated officer (in case of data fiduciary)	Not later than thirty days from the date of receipt
Draft Non-Personal Data Governance Framework	Point 7.7(ii)	Data trustee is obligated to establish grievance redressal mechanisms for the community.		
National Digital Health Mission: Health Data Management Policy	Point 32.2A	Data fiduciary to have effective grievance mechanisms to redress data principals complaints efficiently in a speedy manner	Grievance officer	Data fiduciary to have effective the date of receipt

[52]Cyber Appellate Tribunal remains dormant
[53]A similar kind of regulatory uncertainty is caused in the fantasy sports sector hampering the growth of the sector (Kathuria & Vaidya, 2021)
[54]Similar designation doesn't mean same officer

IT Rules 2021	Part II 3(2)	An intermediary must have a mechanism by which a user or a victim may file a complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it	Grievance officer	Within 24 hours from the receipt of a complaint
Master Direction - Non-Banking Financial Company - Account Aggregator (Reserve Bank) Directions, 2016	Section 11	An account aggregator shall have in place a Board approved policy for handling/ disposal of customer grievances/ complaints	Grievance redressal officer	Not later than thirty days from the date of receipt

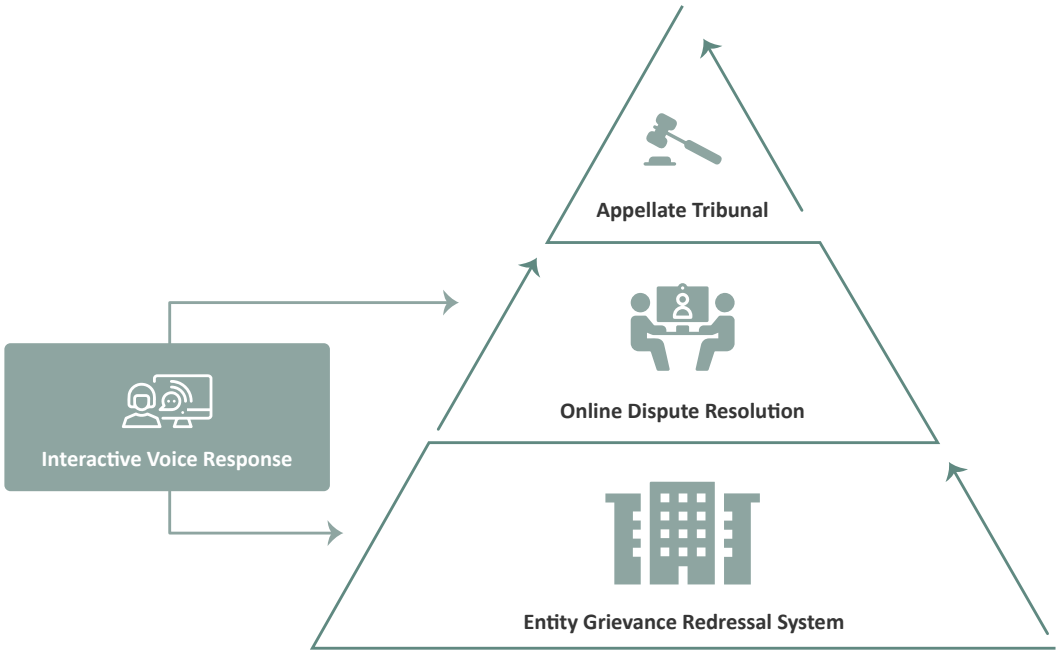
Therefore, as part of the harmonisation process, it is also essential to build capability for a robust grievance redressal mechanism that is both coordinated and agile. The various provisions for grievances as discussed in table 2 have to be smoothened to serve a uniform purpose i.e., data protection.

4.2. CALIBRATED GRIEVANCE MANAGEMENT SYSTEM

Two significant problems with the existing grievance management system are (a) lack of coordination horizontally (in terms of various coexisting systems and mandates) and (b) lack of agility in terms of resolution. Therefore, we suggest a calibrated hierarchical grievance redressal mechanism with horizontal and vertical coordination (between different elements of the system) and agility proofing.

Borrowing inference from the responsive regulation framework (Greenleaf, 2014), the below infographic illustrates the suggested calibrated grievance management system.[55] Moreover, the corrective actions to be taken by any entity within the below grievance management system must follow the enforcement goal alignment principle discussed in Section 3.2.3.

Figure 3: Pyramid eliciting calibrated grievance management system



[55]To implement this system, it is important to amend clause 32 of the PDP bill (JPC has suggested new version titled Data Protection Bill, 2021)

- **Interactive voice response:** The first step in the grievance redressal process is to find the designated portal for lodging a dispute. In many cases, navigating the grievance management system for both consumers and entities is an arduous task making it difficult to reach the designated portal. Therefore, the zero-step of the proposed grievance management system should involve Interactive Voice Response (IVR). This automated voice response system (through call) will navigate consumers (or entities) to reach step 1, i.e. to the entity's grievance redressal system or to step 2, i.e. online dispute resolution if step 1 is already complete.

- **Entity's grievance redressal system[56]:** While various legislations and data sharing/transfer policies mandate entities to set up a grievance mechanism, it is important to harmonise those mandates in terms of point of contact and timeline for resolution. Therefore, step one of the proposed grievance management system is to get the dispute redressed by reporting it to the entity itself.

- **Online dispute resolution:** Online Dispute Resolution (ODR) is a mediated litigant dispute resolution framework facilitated through online platforms. ODR has been extensively used by courts and entities to resolve disputes as this is more efficient, quick turnaround and cost-effective. The ODR framework must be mechanised by DPA, keeping core principles intact (with room for flexibility) in order to reduce its adjudicatory burden. The ODR platform must assign a mediator for every dispute depending upon the nature of the case. Therefore, step 2 of the proposed grievance management system is to reach out to ODR[57] if step 1 fails. In case of step 2 failure, the ODR platform must escalate the dispute to step 3, i.e. moving to the appellate tribunal by automatically filing a complaint with all the details of the negotiation.

- **Appellate tribunal:** Appellate tribunal will be set up under the PDP Bill (chapter XI), which will hear and dispose of any appeal from an order of the adjudicating officer. While the Data Protection Bill, 2021 states that the data principal can reach DPA [Clause 32(4)] with complaints under Clause 69, we suggest this has to be taken up by the appellate tribunal, which has more flavour of the judiciary. In addition to this, we propose a system where the data protection appellate tribunal is horizontally coordinated where benches formed under Clause 71 of the PDP Bill (Clause 72 of JPC's Data Protection Bill, 2021) must comprise other tribunals (regulators if it deems) according to the nature of the dispute. Therefore, step 3 of the proposed grievance management system is the appellate tribunal's verdict if step 2 fails.

5. CONCLUSION

Though India is consistently performing better in terms of ease of doing business, in this paper, we analysed the regulatory complexity and uncertainty for entities in the technology sector. This paper also analysed the state of ad-hoc policymaking, which doesn't keep up with the pace of technology. We also explored how these conflicting and overlapping regulations can have demand-side issues in terms of grievance management.

By analysing the status quo, in this paper, we suggest some strategies for DPA to build a uniform and effective data protection framework for India by smoothening regulations, setting up a Data Protection Board, moving toward responsible regulation and calibrating the grievance management system.

Therefore, as we move over the needle on digitalisation efforts, we believe it is essential to ensure that regulation and grievance management systems are coordinated, updated, and efficient.

[56]It is worth considering a board-based grievance redressal mechanism than a single-point-of-contact based system
[57]Central government was planning to introduce a bill on mediation in the winter session of 2021 (Ahmed, 2021).

Cite this item: Shekar, K. (2022, April). *Building Effective and Harmonised Data Protection Authority - Strategies for Structural Design and Implementation*. The Dialogue.

BIBLIOGRAPHY

- (2019). Report of the Competition Law Review Committee. Ministry of Corporate Affairs. Retrieved from: https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf
- 15 U.S. Code § 57a - Unfair or deceptive acts or practices rulemaking proceedings. (n.d.). Retrieved from Legal Information Institute: https://www.law.cornell.edu/uscode/text/15/57a
- A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority. (n.d.). Retrieved from FTC: https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority
- About Data Empowerment And Protection Architecture (Depa). (n.d.). Retrieved from Indiastack: https://www.indiastack.org/depa/
- Agarwal, S. (2022, April 9). Govt to float new data governance policy framework: Rajeev Chandrasekhar. The Economic Times. Retrieved April 18, 2022, from https://economictimes.indiatimes.com/tech/technology/govt-to-float-new-data-governance-policy-framework/articleshow/90738066.cms
- Ahmed, A. U. (2021). Centre will introduce new law on mediation: Law Minister Kiren Rijiju. Retrieved from Bar and Bench: https://www.barandbench.com/news/law-policy/centre-will-introduce-new-law-on-mediation-law-minister-kiren-rijiju
- Aryan, A. (2021). Looking at 'bigger umbrella', Personal Data Protection Bill likely to include non-personal data. Retrieved from Indian Express: https://indianexpress.com/article/business/looking-at-bigger-umbrella-pdp-bill-likely-to-include-non-personal-data-7552240/
- Banerjee, P. (2021). Digital health IDs face privacy challenge. Retrieved from Livemint: https://www.livemint.com/technology/tech-news/digital-health-ids-face-privacy-challenge-11630867394534.html
- Berman, G., Rosa, S. d., & Accone, T. (2018). Ethical Considerations When Using Geospatial Technologies for Evidence Generation. Retrieved from UNICEF: https://www.unicef-irc.org/publications/pdf/DP%202018%2002.pdf
- Bhardwaj, D. (2021). Centre may tweak IT Act, bring in new penalties. Retrieved from Hindustan Times: https://www.hindustantimes.com/india-news/centre-may-tweak-it-act-bring-in-new-penalties-101631730722211.html
- Brazilian General Data Protection Law. (n.d.). Retrieved from https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf
- Citron, D. K., & Solove, D. J. (2022). Privacy Harms. GWU Legal Studies Research Paper No. 2021-11. https://ssrn.com/abstract=3782222
- Consultation paper on IDEA. Retrieved from Agriculture Cooperation: https://agricoop.nic.in/sites/default/files/IDEA%20Concept%20Paper_mod31052021_2.pdf
- Dvara E-Registry – Leveraging Technology to Enhance Credit and Insurance Delivery to Small and Marginal Farmers in Odisha. (n.d.). Retrieved from Dvara e-Registry: http://www.dvaraeregistry.com/uploads/banner/5ec65b5f9c7a81590057823@Sitaram%20Rao%20Case%20Study.pdf

- EDPB Annual Report 2020. (n.d.). Retrieved from EDPB: https://edpb.europa.eu/system/files/2021-06/edpb_aar_2020_final_27.05.21.pdf
- Eight Lessons to Consider for ODR Implementation. (n.d.). Retrieved from NCSC: https://www.ncsc.org/__data/assets/pdf_file/0020/58016/8-Lessons.pdf
- European Data Protection Board - Rules of Procedure. (n.d.). Retrieved from https://edpb.europa.eu/sites/default/files/files/file1/edpb_rop_version_7_adopted_20201008_en.pdf
- European Data Protection Board. (n.d.). Retrieved from https://edpb.europa.eu/edpb_en
- European Data Protection Supervisor. (n.d.). Retrieved from https://edps.europa.eu/_en
- FTC. (2021). FTC Streamlines Consumer Protection and Competition Investigations in Eight Key Enforcement Areas to Enable Higher Caseload. Retrieved from FTC: https://www.ftc.gov/news-events/press-releases/2021/09/ftc-streamlines-investigations-in-eight-enforcement-areas
- Greenleaf, G. (2014). Asian Data Privacy Laws: Trade & Human Rights Perspectives. Oxford University Press.
- Grover, G., Rajwade, T., & Katira, D. (n.d.). The Ministry And The Trace: Subverting End-To-End Encryption. Retrieved from NUJS Journal: http://nujslawreview.org/2021/07/09/the-ministry-and-the-trace-subverting-end-to-end-encryption/
- Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services including Maps. (n.d.). Retrieved from Department of Science and Technology: https://dst.gov.in/sites/default/files/Final%20Approved%20Guidelines%20on%20Geospatial%20Data.pdf
- How Mobile Vaani Works. (n.d.). Retrieved from Gram Vaani: https://gramvaani.org/?page_id=15
- HT. (2020). RBI seeks exemption from data protection law. Retrieved from Hindustan Times: https://www.hindustantimes.com/india-news/rbi-seeks-exemption-from-data-protection-law/story-kwQzNs614s0C56VK6HTCJP.html
- HT. (2021). Does home ministry want to ban VPN? Here is all you need to know. Retrieved from Hindustan Times: https://www.hindustantimes.com/india-news/does-home-ministry-want-to-ban-vpn-here-is-all-you-need-to-know-101630555850035.html
- India Data Accessibility and Use Policy. (n.d.). Retrieved from MeitY: https://www.meity.gov.in/writereaddata/files/India%20Data%20Accessibility%20and%20Use%20Policy.pdf
- Kapil, S. (2021). Agristack: The new digital push in agriculture raises serious concerns. Retrieved from Downtoearth: https://www.downtoearth.org.in/news/agriculture/agristack-the-new-digital-push-in-agriculture-raises-serious-concerns-77613
- Kapur, D. (2020). Why Does the Indian State Both Fail and Succeed? Journal of Economic Perspective, pp. 31-54. Retrieved from https://www.aeaweb.org/articles?id=10.1257/jep.34.1.31
- Kapur, D., & Khosla, M. (2019). State regulation in India – the art of rolling over rather than rolling back. Retrieved from The Print: https://theprint.in/opinion/state-regulation-in-india-the-art-of-rolling-over-rather-than-rolling-back/216647/
- Kathuria, G., & Vaidya, E. (2021). The Regulation of Fantasy Sports Platforms in India. Retrieved from The Dialogue: https://thedialogue.co/wp-content/uploads/2021/08/Report_Fantasy-Sports-Final.pdf

- Khan, L. M. (2017). Amazon's Antitrust Paradox. Yale Law Review, 564-907.
- Krishnan, S. (2020). Understanding the Indian Regulatory State. Retrieved from EPW: https://www.epw.in/journal/2020/19/book-reviews/understanding-indian-regulatory-state.html
- List of Features/Installations and their sensitive attributes with reference to the "Guidelines for acquiring and producing Geospatial Data and Geospatial Data Services including Maps" . (n.d.). Retrieved from Department of Science and Technology: https://dst.gov.in/sites/default/files/Final%20List%20of%20Negative%20Attributes.pdf
- Mari, A. (2021). Brazil announces national data protection council. Retrieved from ZDNet: https://www.zdnet.com/article/brazil-announces-national-data-protection-council/
- Mariwala, V., & Kwatra, N. (2021). What Mandaviya and Vaishnaw must do. Retrieved from Financial Express: https://www.financialexpress.com/opinion/what-mandaviya-and-vaishnaw-must-do/2318598/
- Market Study On The Telecom Sector In India. (2021). Retrieved from CCI: http://cci.gov.in/sites/default/files/whats_newdocument/Market-Study-on-the-Telecom-Sector-In-India.pdf
- Martin, D. (2018). Pentagon reviews fitness tracker use over security concerns. Retrieved from CBS News: https://www.cbsnews.com/news/pentagon-reviews-fitness-tracker-use-over-security-concerns-fitbit/
- Matthan, R. (2021). The quiet revolution unfolding in data regulation. Retrieved from Livemint: https://www.livemint.com/opinion/columns/data-regulation-is-undergoing-a-significant-revolution-11630945477113.html
- Moss, E., Watkins, E. A., Singh, R., Elish, M. C., & Metcalf, J. (2021). Assembling Accountability. Retrieved from Data & Society: https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/
- NBFC - Account Aggregator (AA) API Specification. (2019). Retrieved from ReBIT: https://api.rebit.org.in/
- Nolan, K. (2018). GDPR: Harmonization or Fragmentation? Applicable Law Problems in EU Data Protection Law. Retrieved from Berkeley Technology Law Journal: https://btlj.org/2018/01/gdpr-harmonization-or-fragmentation-applicable-law-problems-in-eu-data-protection-law/
- ODR: Shifting disputes to resolution. (2020). Retrieved from Agami: https://agami.in/odr/
- Pandey, R., & Patnaik, I. (2016). Legislative strategy for setting up an independent debt management agency. Retrieved from NIPFP: https://edpb.europa.eu/our-work-tools/our-documents/publication-type/rules-procedure_en
- PTI. (2020). Government forms inter-ministerial panel to boost country's capital goods sector. Retrieved from The Financial Express: https://www.financialexpress.com/economy/government-forms-inter-ministerial-panel-to-boost-countrys-capital-goods-sector/2126773/
- Raghavan, M., & Singh, A. (2020). Building safe consumer data infrastructure in India: Account Aggregators in the financial sector (Part–1). Retrieved from Dvara Research: https://www.dvara.com/blog/2020/01/06/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-1/
- Raghavan, M., & Singh, A. (2020). Building safe consumer data infrastructure in India: Account Aggregators in the financial sector (Part–2). Retrieved from Dvara Research: https://www.dvara.com/blog/2020/01/07/building-safe-consumer-data-infrastructure-in-india-account-aggregators-in-the-financial-sector-part-2/

- Rai, S. (2021). India Aims to Open Finance to Millions With User-Data System. Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2021-09-02/india-aims-to-open-finance-to-millions-with-new-user-data-system
- Report Of Competition Law Review Committee. (2019). Retrieved from CCI: https://www.ies.gov.in/pdfs/Report-Competition-CLRC.pdf
- Report of the Financial Sector Legislative Reforms Commission. (2013). Retrieved from GOI: https://www.icsi.edu/media/webmodules/linksofweeks/Volume%20I.pdf
- Ramesh, M. (2021). Why banning cryptocurrencies is bad. Retrieved from The Hindu Businessline: https://www.thehindubusinessline.com/business-laws/why-banning-cryptocurrencies-is-bad/article34352864.ece
- Rizvi, K., & Singh, S. (2021). Does The Traceability Requirement Meet The Puttaswamy Test? Retrieved from Livelaw: https://www.livelaw.in/columns/the-puttaswamy-test-right-to-privacy-article-21-171181
- Robertson, J. (2021). Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role. Retrieved from Bloomberg: https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers
- Robinson, D., Yu, H., Zeller, W. P., & Felten, E. W. (2019). Government Data and Invisible Hand. Retrieved from Yale Law: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1048&context=yjolt
- Roy, S., Shah, A., Srikrishna, B., & Sundaresan, S. (2018). Building State capacity for regulation in India. Retrieved from NIPFP: https://www.nipfp.org.in/media/medialibrary/2018/08/WP_237_2018_0cilwuT.pdf
- Sharma, Y. S. (2021, September 22). niti aayog: Ministries, Niti Aayog oppose draft ecommerce rules. The Economic Times. Retrieved from Economic Times: https://economictimes.indiatimes.com/tech/technology/ministries-niti-aayog-oppose-draft-ecommerce-rules/articleshow/86406643.cms?from=mdr
- Shekar, K. (2021). How to Fight Electoral Fake News on Social Media. Retrieved from Freedom Gazette: https://www.freedomgazette.in/2021/02/how-to-fight-electoral-fake-news-on-social-media/
- Shukla, A. K. (2021). Centre's digital database for farmers under AgriStack programme on off-track mode. Retrieved from Economic Times: https://government.economictimes.indiatimes.com/news/governance/centres-digital-database-for-farmers-under-agristack-programme-on-off-track-mode/83831338
- Sircar, S. (2020). NITI Aayog's New 'India Model' For Personal Data Sharing Explained. Retrieved from The Quint: https://www.thequint.com/tech-and-auto/depa-data-empowerment-and-protection-architecture-niti-aayog-personal-data-sharing
- Suo Moto Case No. 01 of 2021. (n.d.). Retrieved from CCI: https://www.cci.gov.in/sites/default/files/SM01of2021_0.pdf
- The AgriStack: A Primer #SaveOurPrivacy. (2020). Retrieved from Internet Freedom Foundation: https://internetfreedom.in/the-agristack-a-primer/
- Tripathi, A., & V, A. (2021, October 4). A Misplaced Assertion: Harmonisation of Regulations is crucial for the growth of E-Commerce in India. SCC Blog. Retrieved from SCC Online: https://www.scconline.com/blog/post/2021/10/04/a-misplaced-assertion-harmonisation-of-regulations-is-crucial-for-the-growth-of-e-commerce-in-india/

- Why the ODR platform matters for traders. (n.d.). Retrieved from European Commission: https://ec.europa.eu/consumers/odr/main/?event=main.trader.register

- Zanfir-Fortuna, G. (2020). The Complex Landscape of Enforcing The LGPD in Brazil: Public Prosecutors, Courts and The National System Of Consumer Defense. Retrieved from Future of Privacy Forum: https://fpf.org/blog/the-complex-landscape-of-enforcing-the-lgpd-in-brazil-public-prosecutors-courts-and-the-national-system-of-consumer-defense/

The Dialogue™

INFORM ENGAGE IDEATE

https://thedialogue.co

https://www.linkedin.com/company/the-dialogue-india/

@_DialogueIndia

https://www.facebook.com/TheDialogueIndia

@thedialogue_offcial