

RECONFIGURING DATA GOVERNANCE:

Insights from India and the EU

Policy Paper by

Swati Punia, Srishti Joshi, Siddharth Peter De Souza, Linnet Taylor,
Jhalak M. Kakkar, Isha Suri, Arindrajit Basu, Anushka Mittal
(reverse alphabetical order)

INFOGRAPHICS

Ananya Moncourt

DESIGN

Aparna Chivukula



RECONFIGURING DATA GOVERNANCE:

Insights from India and the EU

Swati Punia, Srishti Joshi, Siddharth Peter De Souza, Linnet Taylor, Jhalak M. Kakkar, Isha Suri, Arindrajit Basu, Anushka Mittal
(reverse alphabetical order)

A project of the Tilburg Institute for Law, Technology and Society (Netherlands), the Centre for Communication Governance at the National Law University Delhi, and the Centre for Internet & Society (India)



ACKNOWLEDGMENTS

This report was a collaborative effort between researchers Siddharth Peter De Souza, Linnet Taylor and Anushka Mittal at the Tilburg Institute for Law, Technology and Society (Netherlands), Swati Punia, Sristhti Joshi and Jhalak M. Kakkar at the Centre for Communication Governance at the National Law University Delhi (India) and Isha Suri and Arindrajit Basu at the Centre for Internet & Society, India. The project was funded by ERC Grant number 757247.

Contents

Executive Summary	5
Key Actors in Data Justice Ecosystem	8
Introduction	9
Conceptualising data	11
What is data?	11
Understanding data as a flow (and not as particulate or in binaries)	13
How does data governance emerge beyond data protection?	14
Data Governance	16
Data Governance: Institutional mechanisms and beyond	16
What can the institution of a DPA look like?	17
Data governance beyond the institutional perimeter	18
Case Study of the Indian enforcement institutional landscape	20
Enforcement through formal and informal systems	20
Designing fit-for-purpose Institutions for data governance in India	23
A deep dive on the DPA in India	24
Background of DPA in India	24
Design Analysis of DPBI	25
Operationalizing an inclusive DPBI	29
Conclusion	31

EXECUTIVE SUMMARY

Making Data Governance Work for Data Justice and Empowerment in India and the European Union

This summary presents the conclusions of a workshop held jointly in January 2023 by the Tilburg Institute for Law, Technology and Society (Netherlands), the Centre for Communication Governance at the National Law University of Delhi and the Centre for Internet & Society. The workshop aimed to compare and assess lessons from data governance from India and the European Union, and to make recommendations on how to design fit-for-purpose institutions for governing data and AI in the European Union and India.

Data is not (only) property

Data must be governed for both economic and community interests

Govern for contestability at all levels

Designing fit-for-purpose governance institutions in India



DATA IS NOT (ONLY) PROPERTY

- Data possesses multiple forms of value, each relevant to business, government and society in a different way. However, the governance efforts getting traction nationally are largely driven by the private sector to promote market-centric models of governance where there is emphasis placed on data as an economic commodity.
- The data protection framework and the right to privacy have been co-opted to resolve market related concerns, which effectively excludes the agency of individuals and groups.
- As well as an economic good, data also embodies users' labour, and relations between individuals, groups and institutions. However, the legal regimes seek to give it a definite structure without accounting for competing interests in data regarding representation and justice. This impacts access to justice, and allows capture by powerful stakeholders.

- The lack of a specific non-personal data framework in India allows it to observe the enforcement experience in the EU: particularly the value of thinking in personal/non-personal data binaries, and GDPR's data collection and consent frameworks, where these do not work to protect people, grant access to justice or promote a fair and equitable datafied society (i.e. data justice).



DATA MUST BE GOVERNED FOR BOTH ECONOMIC AND COMMUNITY INTERESTS

- Procedural safeguards for the rights of individuals and groups will never be enough by themselves given the power asymmetries in the digital economy: community-centric and community-driven mechanisms beyond the institutional perimeter are essential to remedy and challenge injustice in the global digital economy.
- However, institutions and procedural frameworks can definitely be a part of a composite solution if deployed effectively. Multi-dimensional justice and accountability mechanisms that include top-down and centralised institutional action as well as diffused, participatory approaches are required.



GOVERN FOR CONTESTABILITY AT ALL LEVELS

- Building an efficient data economy must be balanced by contestability so that data serves the broader public: good governance requires fair and equitable access to justice for every individual to pursue legal remedies. Ensuring this access to justice requires both strengthening legal institutions and meaningfully empowering people by ensuring that they are able to actively participate in problem-solving.
- Access to justice dispensation mechanisms should be made accessible to all individuals regardless of their socio-economic status and identity. An effective enforcement framework is one that works with affected communities to identify problems and craft appropriate measures for harm prevention and redress.
- Enabling people to identify harms and safely navigate the digital space is essential to preventing harms and minimising risks.




DESIGNING FIT-FOR-PURPOSE GOVERNANCE INSTITUTIONS IN INDIA

- The formal enforcement system is slow, complex, and expensive, leading to preference for informal dispute resolution mechanisms. Lok Adalats and Gram Nyayalayas have been underutilised and should be leveraged to support and strengthen formal institutions, because they can help to build trust and confidence and thus make engagement with formal mechanisms less of a hurdle.
- Data protection legislation and enforcement are necessary but insufficient: local-level access points for grievance redressal are essential.
- Establishing the Data Protection Board of India as a quasi-judicial body is insufficient without an accompanying independent regulator. An independent regulator would typically undertake functions such as monitoring, awareness generation and standard setting, and have a mandate to protect people's interests through investigations and suo-moto actions.
- The current structuring, limited functions, and lack of independence of the DPBI may reinforce reliance on approaching traditional appeals courts through writ jurisdiction. This will be inefficient and ineffective because High Court judges often lack the technical expertise to effectively adjudicate data protection issues.
- For accessible and affordable enforcement, the DPBI must build a regional presence through both online and physical offices, and must communicate and collaborate with local-level access points if vulnerable individuals are to have access to grievance redressal and resources for addressing digital harms.



KEY ACTORS IN THE DATA JUSTICE ECOSYSTEM



 Data Justice Ecosystem

- 

GOVERNMENT IS TASKED WITH DEFINING LAW, ARTICULATING POLICY NEEDS AND FRAMING RULES ON DATA PROTECTION AND DATA JUSTICE
- 

JUDICIARY IS TASKED WITH ENSURING THE RIGHT TO PRIVACY, ACCESS TO DATA JUSTICE AND FAIR DATA GOVERNANCE THROUGH LEGAL OVERSIGHT AND INTERVENTION
- 

DATA PROTECTION REGULATOR IS EQUIPPED TO SUPERVISE, MONITOR, INVESTIGATE, INNIATE CASES AND ADJUDICATE UPON DATA PROTECTION RELATED ISSUES.
- 

QUASI JUDICIAL BODY ONLY HAS THE POWER OF ADJUDICATION OVER DATA PROTECTION RELATED COMPLAINTS (E.G. THE DATA PROTECTION BOARD OF INDIA). UNLIKE A FULL-FLEDGED DATA PROTECTION REGULATOR, IT DOES NOT HAVE POWERS OF SUPERVISION, MONITORING AND INSPECTION
- 

PEOPLE PLAY AN ACTIVE ROLE IN THE DATA JUSTICE ECOSYSTEM AND ARE THE PRIMARY ACTORS AFFECTED BY THE DATA ECONOMY
- 

ACADEMIA AND CIVIL SOCIETY PLAY A VITAL ROLE IN FRAMING POLICY DISCOURSE THROUGH RESEARCH, RAISING AWARENESS AND ENCOURAGING ACCOUNTABILITY AMONG ALL STAKEHOLDERS
- 

LAWYERS PROVIDE LEGAL EXPERTISE AND COUNSEL ORGANISATIONS ON COMPLYING WITH RELEVANT DATA PROTECTION LAWS. THEY ALSO COUNSEL AND REPRESENT AGGRIEVED USERS FOR DATA HARMS AND BREACHES
- 

GRASSROOT JUSTICE SYSTEMS ARE INFORMAL SYSTEMS AT A COMMUNITY LEVEL AND PROVIDE A MORE ACCESSIBLE OPTION FOR SECURING JUSTICE. SOME HAVE BEEN FORMALISED THROUGH LAW (GRAM NYAYALAYAS AND LOK ADALATS) AND OTHERS ARE INFORMAL SYSTEMS (INDIA'S COMMUNITY COURTS OR THE EU'S CONSUMER PROTECTION ORGANISATIONS)
- 

PRIVATE SECTOR INSTITUTIONS COLLECT DATA OF PEOPLE IN THE CONTEXT OD PROVIDING THEM DIGITAL SERVICES. SOME INSTITUTIONS HAVE SET UP MECHANISMS TO ENABLE TRANSPARENCY IN HOW USER DATA AND PARTICULARLY COMPLAINTS ARE HANDLED BY PLATFORMS. FOR EXAMPLE SUCH AS FACEBOOK'S OVERSIGHT BOARD
- 

COMMUNITY LEGAL SUPPORT NETWORKS IN THE FORM OF SELF-HELP GROUPS, COMMUNITY PARALEGALS AND LOCAL INFORMATION SHARING NETWORKS ALL AID IN EMPOWERING CITIZENS THROUGH AWARENESS INITIATIVES, OFFERING ASSISTANCE IN FILING COMPLAINTS AND PROVIDING LOCALISED EXPERTISE

Introduction

This policy paper is the result of a workshop organised jointly by the Tilburg Institute of Law, Technology and Society, Netherlands, the Centre for Communication Governance at the National Law University Delhi, India and the Centre for Internet & Society, India. It was titled “Trends in Data Governance in India and the EU” and took place on the 12th of January, 2023. The workshop brought together a number of academics, researchers, and industry representatives in Delhi to discuss a range of issues at the core of data governance theory and practice. At the time of the workshop, various iterations of the final law, DPDP Act 2023 were available for consultation and the participants drew from the concepts already envisaged. The policy paper reports on those critiques along with an analysis of the DPDP Act 2023 that has finally taken shape.

This policy paper collates key takeaways from the workshop by grounding them across three key themes: how we conceptualise data; how institutional mechanisms as well as community-centric mechanisms can work to empower individuals, and what notions of justice these embody; and finally a case study of enforcement of data governance in India to illustrate and evaluate the claims in the first two sections.

In this policy paper we use the term ‘people’ when referring to those affected by the data economy, rather than ‘consumers’, or ‘citizens’. This is because all of us, whether citizens or non-citizens, are continually incorporated in the data economy as both passive and active participants, and data governance must therefore serve our interests under all conditions and degrees of agency. We also use the terminology of ‘data governance’ as distinct from internet governance, which is an important subset of the former but does not cover many uses of data that have implications for rights and justice.¹

The notion of data governance also, importantly, covers uses of data relating to AI and thus points at both current and future governance challenges for the European Union (EU) and India. The workshop touched upon the dynamic and ever-evolving regulatory and institutional landscape of data governance in both jurisdictions. The discussions took a step back to understand, interrogate and apply fundamental questions of data justice which includes examining questions of visibility, representation and autonomy of people in relation to data and discussed how these conceptions should apply to data governance both in India and the EU.²

The two jurisdictions were brought together in a common forum because they are both emergent knowledge-producing jurisdictions with regard to offering frameworks to govern data. In the context of data governance, India and the EU also share their status as sites of

¹ Although data governance and internet governance are often conflated, we treat internet governance as a subset of the former. Much data that matters for social justice issues - particularly data about issues of poverty, discrimination and access to basic needs - is not created on or via the internet, and may not principally reside online. Examples include census data, community data on poverty, or legal processes.

² ‘Global Data Justice’ <<http://globaldatajustice.org/>> accessed 19 April 2021.

contestation among various domestic and international actors including private sector and civil society organisations where governance challenges are emerging on ways to regulate the effects of technology. Both also bear global responsibility in their geopolitical environment when it comes to policy making regarding emerging issues regarding including digital connectivity, value chains and AI among others. Regulations in EU often get exported through the 'Brussels Effect' due to the market power and standard-setting clout wielded by the EU.³ Similarly, policy-making in India with its rapidly growing digital economy and geopolitical position as an exporter of technological solutions could have a ripple-effect in similarly placed emerging economies.⁴

Europe and India are also federal entities, and the division of power is nuanced across multiple axes which makes for distributed frameworks around implementation and enforcement of data governance. One such axis is the separation of powers and competences across the federation and sub federal units. This amounts to the different capacities and priorities for the EU in contrast to the nations which make it up. Similarly, in India, the contest for the capacity to govern data ranges from national to state/sub federal unit legislatures.⁵ In addition to this, tensions remain between different branches of the state in India where separation of power between the executive, judiciary and the legislature also determine how regulation emerges. The paper does not cover the complexity of such variations in competence. However, it is important to highlight these sources for any conversation on data governance in the future.

³ Anu Bradford, *The Brussels Effect* (Oxford University Press, 2020)

⁴ John Reed and Benjamin Parkin, "India plots digital diplomacy push during G20 Presidency," *Financial Times*, January 22, 2023, <https://www.ft.com/content/46760429-a246-4dca-892f-d9a627ea80d7>

⁵ Anushka Mittal, 'Technological federalism: A building block to constitutionalise the digital sphere', (2021) *Economic and Political Weekly* 56(47)

Conceptualising data

The first point of departure and discussion at the workshop revolved around how we should conceptualise data. The rationale for beginning with ascertaining the characteristics of data was to offer different imaginaries beyond seeing data as a commodity that has benefits when it is traded or exchanged. Seeing data beyond its economic characteristics was to afford a discussion about the values and institutional structures which should form the foundation for its governance to understand the implications for data justice. This included conversations around the ways in which people were represented by data, the autonomy that they had to make decisions, and the structural challenges that emerged from engaging in a data economy given the underlying power asymmetries.

As a consequence, we were interested in examining data in terms of the social relations it develops,⁶ in terms of how it represents people, and the cultural, political and epistemic value that it generates.⁷ A further aspect of the characteristics of data was to examine how it emerges, how it is categorised, and to emphasise that it does not just naturally occur but is the result of processing of some kind.⁸ We also wanted to discuss the increasing blurriness of characteristics of data as personal or non personal data as it flows across various entities to result in value.

What is data?

In our conversations around the characteristics of data, we examined the implications of sticking with economic conceptualizations or value-based assessments or the ‘proportification’ of data, and how these offer modes of governance that focus on the market, economic growth, and neoliberal ideas of efficiency.⁹ These arguments emerged in terms of the connection that data has to the profitability of enterprises and its centrality in business models. However, challenges with the enforcement of property rights were also recognized when it came to characterising data as property. This is because property rights mirror the distribution of political and economic power in a society. Similarly, economic value-based assessments of data would only embed the power asymmetries in the digital economy and society and end up empowering corporations at the expense of individuals and groups, especially the most vulnerable. This is because the

⁶ Salomi Viljoen, ‘A relational theory of data governance’, (2021) 131(2) Yale Law Journal, <<https://www.yalelawjournal.org/feature/a-relational-theory-of-data-governance>>

⁷ Lisa Gitelman, Virginia Jackson, ‘Introduction’ in Lisa Gitelman (ed.), “Raw Data” is an Oxymoron (MIT Press 2013)

⁸ danah boyd & Kate Crawford (2012) CRITICAL QUESTIONS FOR BIG DATA, Information, Communication & Society, 15:5, 662-679, DOI: 10.1080/1369118X.2012.678878

⁹ Rob Kitchin, and Lauriault, Tracey, Towards Critical Data Studies: Charting and Unpacking Data Assemblages and Their Work (July 30, 2014). The Programmable City Working Paper 2; pre-print version of chapter to be published in Eckert, J., Shears, A. and Thatcher, J. (eds) Geoweb and Big Data. University of Nebraska Press. Forthcoming, Available at SSRN: <https://ssrn.com/abstract=2474112>

valuation exercise of data for different stakeholders will also mirror the existing asymmetries in society, especially the digital economy.¹⁰ Focusing on economic and value based assessments of data would therefore obscure the lived experience that people have with data, and in doing so, not account for their decisional autonomy to make choices that work in their interest.¹¹

In examining options beyond the economic function of data, our discussions moved to examining the role that data plays in mediating and structuring social relations, addressing questions about who is represented in data, and how to account for individual and group interests. A data justice perspective makes apparent the points at which people in distinct contexts are excluded from digital processes, and how regulation around data needs to account for contestation between people, places and processes as a feature of this mode of regulation.¹² Digitalisation has led to struggles for the adequate and fair representation of both an individual as well as community interests, and the internal power hierarchies that can emerge in attempting to balance such interests.

One participant specifically stated that thinking about data in non-pecuniary terms (agency or empowerment) may not be enforceable in courts due to a lack of jurisprudence.¹³ While theory and discourse grows, real time instances of data-related harms continue and courts remain an important avenue for preventing these harms, largely in search for appropriate frameworks.

Perhaps a solution to this challenge lies in accepting that individuals and communities have economic, social and cultural rights in data, which should be incorporated in the conceptualisation of data itself.¹⁴ For example, a worker in the gig economy would have a right against the processing of their data being used to calculate performance and deny basic labour rights like minimum wage. This apportions the material value or the propertarian nature of data beyond the powerful private actor to ensure autonomy of other stakeholders in securing fundamental rights.¹⁵

While the consensus on the most appropriate framing of data was not achieved, a method of elimination was used to make a case for the pitfalls of the framings being implicitly and explicitly used in data laws. At the moment, the infrastructure and architecture around data is created

¹⁰ Seeta Peña Gangadharan & J drzej Niklas (2019) Decentering technology in discourse on discrimination, *Information, Communication & Society*, 22:7, 882-899,

¹¹ Lina Dencik, Arne Hintz, Joanna Redden & Emiliano Treré (2019) Exploring Data Justice: Conceptions, Applications and Directions, *Information, Communication & Society*, 22:7, 873-881

¹² Linnet Taylor, 'What is data justice? The case for connecting digital rights and freedoms globally' (2017) 4(2) *Big Data & Society*

¹³ "Regulating Data as Property: A New Construct for Moving Forward" by Jeffrey Ritter and Anna Mayer (duke.edu)

¹⁴ Stephanie Russo Carroll and others, 'The CARE Principles for Indigenous Data Governance' (2020) 19 *Data Science Journal* 43.

¹⁵ Siddharth Peter de Souza, 'The Performativity of Ratings in Platform Work' (Centre for International Governance Innovation) <<https://www.cigionline.org/articles/the-performativity-of-ratings-in-platform-work/>> accessed 2 October 2022.

such that the issue of what data actually is is not clarified but left to take a suitable shape, as determined by stakeholders or exogenous circumstances. Given this ambiguity, the participants agreed that there is a sense of urgency in the legal conceptualisation of data to enforce contestability in fora such as courts. It also requires that civil society and lawmakers use the lens of political economy to decide how data's value is distributed, to whom and how.¹⁶

Understanding data as a flow (and not as particulate or in binaries)

While the exact conception of data is being mulled over, both jurisdictions have provided typologies to understand data. There are various configurations of data which are used such as personal and non-personal data. However, the legal regimes and contextual significance of such terms is vastly different.¹⁷ This is reflected in the EU Regulation on a framework for the free flow of non personal data which focuses on harmonisation and free flow of non personal data across the EU, defined as 'data other than personal data'.¹⁸ India considered various policy approaches to non personal data and the first significant instance emerged in the form of the Expert Committee Report on Non Personal Data Governance Framework, which sought to classify certain non-personal datasets as public, to be governed and managed by amorphously outlined/fluid communities.¹⁹ A separate legal framework for non-personal data was discarded and instead made a part of the iterations of the data protection law under consideration and subsequent data sharing policies.²⁰ In all these changes, the framing and presence of community rights to data have been completely obliterated. At the moment, none of these regulatory ideas are in force. Further, the DPDP Act 2023 makes no reference to non-personal or anonymised data. In its absence arises an opportunity for academics and civil society to determine the principles and values which should underpin governance in this sphere.

The comparison between the EU and India, in this space, indicates the vast difference in the way non-personal data is characterised. It highlights the different data governance principles

¹⁶ Amber Sinha and Arindrajit Basu, 'Why Metaphors for Data Matter' (Bot Populi) <https://botpopuli.net/?post_type=post&p=4069> accessed 11 September 2023.

¹⁷ Vidushi Marda, 'Non-personal data: the case of the Indian Data Protection Bill, definitions and assumptions', (Ada Lovelace Institute, 15 October 2020) <<https://www.adalovelaceinstitute.org/blog/non-personal-data-indian-data-protection-bill/>> accessed 23 February 2023

¹⁸ Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data in the European Union [2018] OJ L 303

¹⁹ Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework*; Amber Sinha, Arindrajit Basu, 'Community Data and Decisional Autonomy: Dissecting an Indian Legal Innovation for Emerging Economies' (CIS, 24 May 2021) <<https://cis-india.org/internet-governance/blog/community-data-and-decisional-autonomy-dissecting-an-indian-legal-innovation-for-emerging-economies>> accessed 2 March 2023

²⁰ Ministry of Electronics and Information Technology, National Data Governance Framework Policy (Draft)

that the jurisdictions employ to attach value and significance to a specific type of data. Such differences are also important to note for any work on distilling a common regime for global data governance. There is a technological consensus that data takes on different characteristics at different stages of processing.²¹ In this regard, a new paradigm should be examined to take into account such non-binary nature of data and it should be examined as a flow that also incorporates relationships and various forms of agency.

How does data governance emerge beyond data protection?

It was observed that data governance, especially questions about its collection, use and distribution, is shadowed by the discourse and discussion on privacy. While, it is a right of immense importance, the shaping of the data protection frameworks in the discourses on data governance has weaponized privacy to the occlusion of empowerment and agency.²² Privacy is translated into an interest that can be traded based on market forces rather than an inalienable right that the state is duty-bound to protect. This came across clearly in the intervention of one participant who commented on some of the fundamental failings of the consent model in the GDPR in the European Union. Consent has been one of the weak points of GDPR. It has become a way for service providers to assert legal compliance while side-stepping the problem of explaining how data collection, use and re-use will actually affect people - mainly because the possible uses of data have evolved to the point where data's lifecycle is not predictable for the platforms or service providers who originally collect it. Because of the lifecycle problem with data, consent-based approaches also have ended up protecting the most powerful economic interests, i.e. those with the greatest resources and technical capacity, who can translate data into different functions and use it most effectively as a form of capital.²³ The process of providing consent is rarely a fair negotiation but usually plays out as one-sided standard form contracts that are difficult to meaningfully comprehend. This has been central to the inequity present in the present data protection system where control over the value of data is provided to corporations. In the DPDP Act 2023, the burden of ensuring privacy is on the individual who can also be denied services in the absence or revocation of consent. The law recognises the need for data to move around to generate value (much like capital) and provides points of pauses to be individually exercised by principals. It is considered as a unit for individuals but as a flow for other actors. The inability to bargain or conceive distinct imaginations in the digital economy is thus commonly seen in emergent jurisdictions also.

²¹ Michèle Finck, Frank Pallas, 'They who must not be identified—distinguishing personal from non-personal data under the GDPR', (2020) *International Data Privacy Law*, 10(1)

²² Geoffrey A. Fowler, "At CES, Apple, Facebook and Amazon are preaching privacy. Don't believe the hype." *Washington Post*, January 08, 2020, <https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/>

²³ Shoshana Zuboff, *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*, (First edition PublicAffairs 2019)

This highlights the difference between information privacy and real agency with regard to data. These insights are important to consider to determine the scope of alienability of the right to privacy, both by public authorities and private service providers.

Even on a global level, there are efforts to promote data collection and not rethink the current mechanisms. This is done directly through technological design but also using rather indirect means of WTO trade agreements. For instance, the plurilateralisation of trade agreements at the WTO has formed a way to destabilise the status quo of e-commerce negotiations at the WTO. A small number of developed countries, through the Joint Statement Initiative on E-commerce, wish to ensure data flows are without restrictions or regulations.²⁴ This significantly reduces the space for developing countries who are not involved in the negotiations. Eventually they must accept the outcomes that they do not participate in to succeed in the new status quo. This is in accordance with the current conceptualisation of data where rights tend to be named in data legislation but not meaningfully enforced (especially on the collective level), because this does not fit with the fundamentally economic framing of data governance.

Similarly, privacy has often become an instrument of top-down power rather than bottom-up contestability. Privacy-washing is ubiquitous in the EU, where actors perform compliance and consent while in reality their exploitative practices only remove power from individuals and communities rather than strengthening their agency. In India however, the lack of a comprehensive data protection law up to this point has meant there has been no clear incentive to even be a privacy preserving jurisdiction, and the culture of digital consent has not been created. In the DPDP Act, 2023 the notion of 'deemed consent' removes the data subject from the picture, posing a different challenge to the notion of data subject empowerment where the notion of conscious choice and consent is dismissed. Both the EU and Indian approaches therefore have serious drawbacks, but are part of a worthwhile debate about how to move away from hyper-individualised consent-based approaches, which are marred by information asymmetry between people and processors, and lack of digital literacy. Consequently, alternate approaches rooted in the more collective management of data were proposed. Models such as data stewardship, data commons and community-driven approaches to data governance were endorsed by several participants in this context. Some participants suggested that representation models need to be reviewed and updated to allow for fairer negotiations through intermediaries. While the concept of consent managers has been included expressly in the law in India, the basis of the relationship between the data principal and the intermediary is again driven by individualised notions which do not account for alternate models adequately.

²⁴ WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore 20 January 2023 <https://www.wto.org/english/news_e/news23_e/igo_20jan23_e.pdf> accessed 4 April 2023

Data Governance

Data Governance: Institutional mechanisms and beyond

Society, both domestically and globally is structured by hierarchy and power differentials. Public institutions are not independent of these dynamics but instead are often shaped by the powerful.²⁵ The rules and principles they create are often designed to protect the interests of the powerful. At the same time, due to public participation and public-facing accountability, institutions have also been designed to serve the vulnerable and marginalised.²⁶ Modern day jurisprudential approaches to 'transformative constitutionalism' views the state, not as a neutral non-interfering observer into the daily lives of individuals and communities, but as an active participant in the quest to fight structural inequality and injustice.²⁷

These societal power hierarchies are augmented in the case of digital economies. Entities and select individuals controlling data can exploit data and related infrastructure to control the lives of people whose data they hold in addition to concentrating their own wealth and capital. For Pistor, "lawyers can convert about any asset into capital,"²⁸ including personal data that should be rightfully controlled by individuals. This can be seen in effect when one analyses the way rights, access and use to data is structured for people as compared to data fiduciaries or processors in the data protection framework in India. Institutional design and an active welfare state that protects the data of individuals and communities are therefore essential. However, institutions tend to replicate technical, political and social power, which means that they will rarely be necessary and sufficient. Individuals will always face challenges in accessing institutions riddled with lack of independence, capacity constraints and focused predominantly on wealth-seeking motives rather than justice.

A practical case study at the workshop revolved around the question of whether India was ready for a Data Protection Authority (DPA).²⁹ The debate revolved mostly around the institutional framework for enforcing data protection. This is discussed in detail in the next section.

²⁵ Michael E. Levine and Jennifer L. Forrence, "Regulatory capture, Public Interest and the Public Agenda: Toward a synthesis" *Journal of Law, Economics and Organization* Vol. 6

²⁶ John Rawls, *A Theory of Justice* (Harvard University Press, 1971)

²⁷ See Gautam Bhatia, *The Transformative Constitution: A radical biography in nine acts* (Harper Collins, 2019)

²⁸ Katharina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton University Press, 2019)

²⁹ Anirudh Burman, "Resisting the Leviathan: The Key Change in India's New Proposal to Protect Personal data," *Carnegie India*, November 28, 2022, <https://carnegieindia.org/2022/11/28/resisting-leviathan-key-change-in-india-s-new-proposal-to-protect-personal-data-p-ub-88496>

What can the institution of a DPA look like?

Participants stated that in other jurisdictions such as the EU, individuals have found it difficult to access tribunals easily and have often had their claims and grievances left unaddressed. This is due to two significant challenges, including lack of resources for a national level DPA and forum shopping for lenient DPAs.³⁰ As a consequence of these challenges, only limited jurisdictions, particularly Ireland and Luxembourg, have had to deal with the most significant data protection cases within the EU.³¹ Unfortunately, this only exacerbates the issue of lack of resources. One of the suggested solutions to address the issue of forum shopping has been to establish a strong central authority that only decides cases involving big actors. This could help mitigate forum shopping for lenient DPAs.

In addition to regulatory capacity, lack of adequate accountability mechanisms in India was highlighted as a reason for refraining from establishing a DPA in India. It was posited that due to these reasons regulatory institutions have therefore become an excuse for cementing market power rather than an avenue for justice that can be easily accessed by individuals.

Several other participants presented a more optimistic view of regulatory institutions. While capacity challenges were acknowledged, some argued that a multi-stakeholder ecosystem driven approach to regulation could be used to mitigate some of the capacity driven challenges. Further, several alternatives to tribunal driven mechanisms such as data ombudspersons and a cap and trade system for data credits (like for carbon emissions) were advanced. Another mooted solution was collective lawsuits being launched by Consumer Protection Organisations (CPOs) in the EU as being effective in representing people collectively and challenging the dominance of big tech companies. Such lawsuits are more feasible than individual claims, which usually result in the claimants being buried in paperwork. It was discussed that collective lawsuits of this nature interestingly provide the option of collective action in private enforcement of a data subject's right. However, as these models have not yet been elaborated in academic research or in policy, evidence-driven research evaluating these models may be useful before recommending these for policy implementation.

Some participants envisaged the regulator to have ex-ante powers similar to some other regulators in the country such as the Telecom Regulatory Authority of India (TRAI) or Securities and Exchange Board of India (SEBI) along with some quasi judicial powers. Amongst EU member States several countries such as Finland, Sweden, Ireland have emphasised on the preventive and proactive role of the DPAs through ex-ante powers. Whereas, certain member countries including Latvia, Czech Republic, and Greece have prioritised ex-post enforcement by DPAs which largely oversees compliance with data protection legislation. Almost all participants flagged that the

³⁰ European Data Protection Board, "Lack of resources puts enforcement of individuals' data protection rights at risk," September 17, 2022, https://edpb.europa.eu/news/news/2022/lack-resources-puts-enforcement-individuals-data-protection-rights-risk_en

³¹ Foo Yun Chee, "Ireland, Luxembourg need more muscle to police tech giants, EU report says," Reuters, January 23, 2020, <https://www.reuters.com/article/us-eu-privacy-gdpr-idUSKBN23U2U5>

current constitution of the DPBI as per the DPDP Act lacks independence and is far from ideal. Additionally, the Board has been envisaged as a quasi judicial body rather than as a regulator. Lack of independence impedes the ability of DPAs to function effectively since they lack autonomy to carry out their tasks, and may also lack powers to investigate, intervene in processing operations, offer legal advice and engage in legal proceedings.

A further point to note is that the role of data protection supervisory authorities is also likely to change with the growth of the impending AI economy with the risks pointed out earlier increasing significantly with the volume and velocity of complaints. In addition to dealing with compliance related issues, data protection authorities will be compelled to engage with the impact of new and emerging technologies on fundamental rights and will play a critical role in protecting against the erosion of individual self-determination by the private sector. The past decade has witnessed unprecedented breakthroughs in AI due to an increasing availability of bandwidth for data transfer, data storage and computational resources along with progressive datafication enabling new forms of data management.³² The current state of the art suggests that AI relies heavily on data processing and raises legitimate concerns on the adequacy of existing data protection regulations in addressing these issues.³³ Some of these include principles of fairness (biased datasets leading to arbitrary discrimination), purpose limitation (use of data for a purpose it was not originally collected for), data minimisation (AI requires large amounts of data including personal data) and transparency (black box makes it hard to explain how information is correlated and weighted in a specific process).³⁴ These challenges necessitate investments in regulatory capacity to ensure that data protection authorities are adequately equipped to mitigate the harms posed by existing and emerging technologies including AI.

Given the state of technological pace and its impact on a multitude of rights, it is difficult to create a single body having the resources to deal with this phenomenon not limited to consumer protection, freedom from discrimination, antitrust, and freedom of speech and expression.

Data governance beyond the institutional perimeter

Participants stressed that it is critical for us to think of models of data governance beyond institutions and legal claims in terms of rights. 'Justice' is not just about having institutions or rules in place but about thinking through how these institutions and rules exist (entrench or reduce) power asymmetries in the broader scheme of social relations.

As discussed in the previous section, there was overarching acknowledgment of the notion that data protection will not account entirely for the gamut of issues raised within the context of

³² Council of Europe, Artificial Intelligence and Data Protection, <https://rm.coe.int/prems-192119-gbr-2051-lignes-directrices-sur-l-intelligence-artificiel/1680a4ca4a>

³³ Ibid.

³⁴ Datatilsynet, "Artificial intelligence and privacy," Report January 2018, <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf><https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>

data justice. Therefore, we must think about accountability mechanisms beyond institutional frameworks that are designed and implemented either by the state or the private sector such as data held and governed by public data trusts or through data commons.³⁵

For example, the Te Hiku, a Maori tribe in New Zealand built their own digital hosting platform to protect their language. As new technologies tend to use only western languages, speakers of traditional languages had to either adopt a dominant language or forego larger opportunities in the culture and economy.³⁶ Private actors using existing technological models and protocols were following rules set by existing data governance institutions. The legal constructs and institutional framework was not violated, yet the identities and aspirations of marginalised communities were undermined. This underscores the need for communities to think beyond institutional perimeters to construct values, norms and infrastructures that can work for their communities. Scientists who join the Te Hiku platform have to abide by a decision-making framework based on Maori values and principles and cannot do what they see fit with the data. Data sovereignty, in this case, is collectively good for this community, and a means to resist institutions created by nation-states and shaped by companies.

Traditional (western) notions of sovereignty are state-centric rooted in control over territory.³⁷ However, sovereignty and its use in international law was a legal construct used by European settlers to legally justify the appropriation of land from indigenous inhabitants through territory driven visions of sovereignty and control. Sovereignty, in the western territorial sense, did not describe the relationship between indigenous communities and their land - a relationship rooted in care, not exploitation or control. However, given the reorientation of entrenched norms and global discourse along Westphalian territorial lines, indigenous communities have now begun to reassert their rights to self-determination and autonomy by reclaiming the use of sovereignty and its social construction.

In the next section, we undertake a case study of the Indian context and engage with the institutional structures for data protection as well as community initiatives that may be valuable in enabling data justice and complementing the work of formal systems.

³⁵ "Governing data and artificial intelligence for all: Models for sustainable and just data governance," European Parliament Research Service, [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU\(2022\)729533_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf). [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU\(2022\)729533_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729533/EPRS_STU(2022)729533_EN.pdf)

³⁶ Karen Hao, "A new vision of artificial intelligence," MIT Technology Review, April 22, 2022, <https://www.technologyreview.com/2022/04/22/1050394/artificial-intelligence-for-the-people/>

³⁷ Barker argues that "... sovereignty is historically contingent. There is no fixed meaning for what sovereignty is – what it means by definition, what it implies in public debate, or how it has been conceptualized in international, national or indigenous law. Sovereignty – its related histories, perspectives, and identities – is embedded within the specific social relations in which it is invoked and given meaning. How and when it emerges and functions are determined by the "located" political agendas and cultural perspectives of those who rearticulate it into public debate or political document to do a specific work of opposition, invitation, or accommodation" See Joanne Barker, "For who sovereignty matters," in Joanne Barker (eds) *Sovereignty Matters: Location of Contestation and Possibility in Indigenous Struggles for Self-Determination* (University of Nebraska Press, 2006) 31

Case Study of the Indian enforcement institutional landscape

India's digital growth story is made of contrasting realities. It is incubating the world's third largest startup ecosystem,³⁸ expanding due to a large pool of talented youth in the IT sector. At the same time, a rapidly growing digital footprint is widening the digital divide while also bringing a large number of new, inexperienced, young, and vulnerable groups of people within the fold of the internet. A considerable portion of the population coming onto the internet have low levels of general literacy and lack the much needed digital literacy skills to safeguard themselves from risks and online harms.³⁹ There are significant disparities in digital skills levels between different age groups, gender, education levels, income brackets and regions.⁴⁰ Ability to use the internet in rural areas, as reported by the 75th Round Report of the National Statistics Survey, stands at only 13%, significantly lower than the 37% in urban areas.⁴¹ Researchers have also pointed to the chasm that exists within urban areas between those who can adequately access and use the internet and those who cannot.⁴² This raises fundamental questions of equity and inclusion of access to justice for harms arising in the context of data protection for marginalised and vulnerable groups. This section explores the various mechanisms which are available to the people to govern data.

Enforcement through formal and informal systems

In India, the constitutional obligation of equal treatment under the law is coupled with the State's responsibility to offer legal assistance to the economically disadvantaged. The State's responsibility to ensure access to justice was historically limited to the creation of impartial laws and the right of individuals to defend themselves in court. However, with the introduction of Article 39A in 1976 to the Constitution, the right of economically disadvantaged individuals to free legal assistance came to be protected. Despite being a step towards bridging the justice gap, it has struggled to narrow the divide in practice, and both formal and informal systems of justice

38 BL Mumbai Bureau, 'Despite Funding Winter, India Is the Third Largest Startup Ecosystem Globally: NASSCOM' (BusinessLine, 15 February 2023) <<https://www.thehindubusinessline.com/info-tech/despite-funding-winter-india-is-the-third-largest-startup-ecosystem-globally-n-asscom/article66513083.ece>> accessed 18 August 2023.

39 'Data Protection and Digital Rights in India | IDR' (India Development Review) <<https://idronline.org/article/rights-data-protection-and-digital-rights-in-india/>> accessed 18 August 2023.

40 IAMA and Kantar, 'ICUBE 2020: Internet Adoption in India' (2021) <https://images.assettype.com/afaqs/2021-06/b9a3220f-ae2f-43db-a0b4-36a372b243c4/KANTAR_ICUBE_2020_Report_CI.pdf> accessed 18 August 2023.

41 National Statistics Office, 'Household Social Consumption on Education in India - 75th Round' (2017) NSS Report No. 585(75/25.2/1) <https://mospi.gov.in/sites/default/files/publication_reports/Report_585_75th_round_Education_final_1507_0.pdf> accessed 18 August 2023.

42 Akhilesh Patil and Dhruv Shekhar, 'Offline and Falling Behind' (2019) XXXVIII <https://www.commoncause.in/publication_details.php?id=624> accessed 18 August 2023.

face significant challenges.⁴³

Formal systems of enforcement in India have been plagued with challenges of being slow in resolving disputes, complex to navigate and expensive.⁴⁴ According to a 2017 study in India, formal enforcement systems (courts and the police) constituted the least preferred form of conflict resolution, citing reasons of affordability, accessibility and efficiency.⁴⁵ Informal and non-judicial mechanisms such as family, friends, village elders, or caste or religious panchayats were preferred for resolving serious disputes. India has a long-standing tradition of resolving disputes through conciliation efforts outside of the formal legal system.⁴⁶

Lok Adalats⁴⁷ and Gram Nyayalayas⁴⁸ are novel examples of institutionalising informal dispute resolution mechanisms to ensure people have access to justice at their doorstep and no one is denied justice due to a social, economic and other disability.⁴⁹ However, their adoption has been unsteady and largely inconsistent. Lok Adalats have gradually failed to provide the swift and fair justice upon which people had come to rely.⁵⁰ This was possibly due to formalised structures and processes being reinforced in the Lok Adalats, thereby disregarding the intention behind their establishment - that is, providing a set up for making legal settlements accessible. Besides this, other factors such as poor relationship between judges and lawyers, unpreparedness, and pressure to settle have also added to its slow adoption.⁵¹ Some suggest that poor adoption of Lok Adalats is possibly due to burdens of formal systems introduced which are inconsistent with its design and objective.⁵² As of 2021, only ten states have adopted and operationalised 256 Gram

⁴³ Dasra, 'Tipping the Scales - Strengthening Systems for Access to Justice in India' <<https://clapindia.org/profile/5cc81eb1c0c43.pdf>>.

⁴⁴ Khaitan Nitika, Seetharam Shalini and Chandrashekar Sumathi, 'Inefficiency and Judicial Delay: New Insights from the Delhi High Court' (Vidhi Centre for Legal Policy 2017) <https://vidhilegalpolicy.in/wp-content/uploads/2020/06/InefficiencyandJudicialDelay_Vidhi-1.pdf>.

⁴⁵ Aarefa Johari, 'The Indian Justice System Is Too Slow, Too Complex and Too Costly, Says New Study' [2018] Scroll.in <<https://scroll.in/article/866158/the-indian-justice-system-is-too-slow-too-complex-and-too-costly-says-new-study>> accessed 18 August 2023.

⁴⁶ Sarfaraz Ahmed Khan, *Lok Adalat: An Effective Alternative Dispute Resolution Mechanism* (APH Publishing 2006).

⁴⁷ Constituted under the Legal Services Authorities Act, 1987.

⁴⁸ Gram Nyayalayas were formalised through the Gram Nyayalaya Act, 2008. The predecessor for the Gram Nyayalayas were the Nyaya Panchayats, which were initially tasked with the responsibility of providing access to justice at the village level.

⁴⁹ Chauhan, 'Origin & Evolution Of Lok Adalat System In India – The Dispatch' (14 January 2022) <<https://www.thedispatch.in/origin-evolution-of-lok-adalat-system-in-india/>> accessed 18 August 2023.

⁵⁰ Jayanth Krishnan and Marc Galanter, 'Bread for the Poor: Access to Justice and the Rights of the Needy in India' [2004] 55 *Hastings Law Journal* 789 (2004) <<https://www.repository.law.indiana.edu/facpub/380>>.

⁵¹ Ibid.

⁵² Ibid.

Nyayalayas.⁵³ While Lok Adalats have a comparatively better adoption rate than Gram Nyayalayas, there has been a decline in the efficacy of Lok Adalats particularly because of the severe lack of resources which prevent adequate administration of these bodies.⁵⁴

Outside of the formal court system, India has informal courts and councils working at the grassroots level to provide access to justice in remote and rural areas. It is also important to examine the role of such informal and indigenous systems of justice in India, particularly the role of the "community" within these systems. Community Courts and Mahila Panchayats have been established in rural areas to ensure that they serve as the first point of contact for people seeking justice. With the intention of being easily accessible, affordable and an alternate forum for individuals to bring forward their grievances, these institutions have been helpful in building last-mile access to justice for the vulnerable and marginalised who often find it difficult to access formal systems of justice dispensation. Many reports highlight the effectiveness of informal institutions in resolving common problems in rural areas, from small boundary disputes to marital issues.⁵⁵

Informal justice systems are built on community values and traditions. They tailor approaches according to cultural norms keeping the best interests of the community at the heart of problem-solving.⁵⁶ Hence, participation of the community is encouraged in decision making and is key to enforcing solutions. Inadvertently, this also leads to enhancing legal awareness and empowerment of the people of the community. For instance, forest conservation programmes harness the power of the relationship building between different actors of the ecosystem (police and elders of the community) to understand systemic problems and draw remedies/solutions with the local community to ensure effective implementation.⁵⁷ While the recently passed law has a formal Data Protection Board set up as a quasi judicial mechanism, it would be useful to draw on past experiences and empower various informal community based institutions to ensure that individuals in rural areas, from marginalised and vulnerable communities, etc. are made aware of their rights and protections under the law and are aware of the formal institutional mechanism they can use to raise complaints of data breaches and violations. We suggest some such mechanisms later in this policy paper to ensure formal institutions have last mile access.

⁵³ Press Information Bureau, '256 Gram Nyayalayas Operational in 10 States' <<https://pib.gov.in/PressReleasePage.aspx?PRID=1782616>> accessed 18 August 2023.

⁵⁴ Tameem Zainulbhai, 'Justice for All: Improving the Lok Adalat System in India' (2016) 35 Fordham International Law Journal

⁵⁵ E-Pathshala, 'Access to Justice' <https://epgp.inflibnet.ac.in/epgpdata/uploads/epgp_content/Law/02._Access_to_justice/05._Informal_Access_to_Justice/et/5632_et_05ET.pdf>.

⁵⁶ UNDP, UNICEF and UN Women, 'Informal Justice Systems: Charting a Course for a Human Rights-Based Engagement - A Summary' <<https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2013/1/Informal-Justice-Systems-Summary.pdf>>.

⁵⁷ Ranjay K Singh and others, 'Classification and Management of Community Forests in Indian Eastern Himalayas: Implications on Ecosystem Services, Conservation and Livelihoods' (2018) 7 Ecological Processes 27 <<https://ecologicalprocesses.springeropen.com/articles/10.1186/s13717-018-0137-5>> accessed 18 August 2023.

These systems should not be considered a complete replacement for formal systems of adjudication but complementary strategies that help build meaningful access to justice in the ecosystem. An effective solution requires nuanced and contextual understanding of the problem that requires informal mechanisms.

While informal institutions such as the Lok Adalats and Gram Nyayalayas have been formalised through statutes having powers akin to civil courts and to pass binding decisions, there remain many kinds of informal systems whose decisions are not enforceable in the court of law. Informal justice systems have been criticised for perpetuating social inequalities and discriminating against vulnerable and marginalised sections of rural areas, and for being susceptible to abuse of power, corruption and a lack of legal expertise.⁵⁸

Designing fit-for-purpose Institutions for data governance in India

Strengthening systems of enforcement requires a blend of accessible, affordable and comprehensible laws and legal systems.⁵⁹ For designing meaningful access to justice in the digital world, relevance and efficiency of existing infrastructure, community-level initiatives, and decentralised models of justice should be assessed. Rather than providing band-aid solutions to fix the justice gap, the enforcement mechanisms in the digital landscape ought to be tailored keeping in mind the role informal and ancillary institutions can play. While formal systems are indispensable, there are serious concerns of accessibility, affordability and efficiency. Supplementing formal systems of enforcement with ancillary informal or grassroots level systems can provide more sustainable and efficient ways of resolving disputes as well as help democratise the enforcement system.

The community is a driving force in India, and capturing that understanding and harnessing this element can help design justice solutions that allow people to resolve issues effectively, regardless of their economic standing. Our formal dispute resolution and justice delivery institutions are riddled with pre-existing challenges of being slow, heavily burdened, and expensive. This may act as a barrier to the economically weak, marginalised and those with low digital literacy to approach such forums to seek redressal of their grievances. Given this, it is crucial to identify efficient local community-level initiatives and plug the gaps through structural reforms that help strengthen the foundations of justice dispensation in India. We suggest some such mechanisms later in the policy paper.

The decentralised governance that has taken shape in India after the introduction of the 73rd and 74th amendments to the Constitution of India, has proven to be one of the more

⁵⁸ Kalindi Kokal, 'Hope for Justice' (2013) 48 Economic & Political Weekly <<https://www.epw.in/journal/2013/45-46/commentary/hope-justice.html>> accessed 18 August 2023.

⁵⁹ Dasra, 'Tipping the Scales - Strengthening Systems for Access to Justice in India' <<https://clapindia.org/profile/5cc81eb1c0c43.pdf>>

successful aspects of India's democratic experiment. These amendments have led to deepening of democracy, political inclusion and participation in self-governance by marginalised sections of the society.⁶⁰ Esther Duflo and Raghavendra Chattopadhyay, in a field study involving the working of Panchayati Raj Institutions in West Bengal and Rajasthan observed that women's representation in the local bodies has had a net positive impact on the delivery of local public goods to marginalised communities.⁶¹ Evidence has also emerged to state that decentralised governance has led to increased participation from members of marginalised communities such as women, Scheduled Castes (SC) and Scheduled Tribes (ST).⁶² Given the success of community centric/ driven systems and the proposed online grievance redressal mechanism under the DPDP Act, it would be essential to develop linkages between the two.

A crucial element of good governance and advancing societal progress is the provision of fair and equitable access to justice for every individual to pursue legal remedies. To ensure universal access to justice, it is crucial to not only strengthen legal institutions but to meaningfully empower people by ensuring that they are able to actively participate in problem solving. Access to justice dispensation mechanisms should be made accessible to all individuals regardless of their socio-economic status and identity. It is necessary therefore that an effective enforcement framework works with the community affected to identify the problems and craft appropriate measures for prevention and resolution of harm. Concurrently, enabling people to identify harms and safely navigate the digital space is essential to preventing harms and minimising risks. At the moment, DPDP Act is assessed below to understand how it promotes access to justice and the way it can be designed better.

A deep dive on the DPA in India

Background

In the context of data governance, the learnings and experiences distilled from the formal and informal mechanisms can be utilised to ensure protection that works for all. In the absence of comprehensive data protection legislation, issues pertaining to data justice in India have traditionally been handled by the judiciary through interpretation of constitutional provisions

⁶⁰ Niranjana Sahoo and Keerthana Chavaly, 'Decentralisation @75: How the Third-Tier Institutions Have Deepened India's Democracy?' (ORF) <<https://www.orfonline.org/expert-speak/decentralisation-75-how-the-third-tier-institutions-have-deepened-indias-democracy/>> accessed 18 August 2023.

⁶¹ Raghavendra Chattopadhyay and Esther Duflo, 'Impact of Reservation in Panchayati Raj: Evidence from a Nationwide Randomised Experiment' (2004) 39 Economic and Political Weekly 979 <<https://www.jstor.org/stable/4414710>> accessed 18 August 2023.

⁶² DownToEarth Staff, 'Who Has Rights over a Citizen's Body? New Twist in Aadhaar Controversy' DownToEarth (3 May 2017) <<https://www.downtoearth.org.in/news/governance/who-has-rights-over-citizens-body-new-twist-in-aadhaar-controversy-57754>>.

and judicial pronouncements.⁶³ The DPDP Act provides for the establishment of the DPBI which is envisaged to be a quasi-judicial body, with a limited mandate as compared to a full fledged regulator discussed in the previous iterations of the proposed law.⁶⁴

In order to ensure effective functioning of the DPBI, building trust and dependability in the institution is crucial to ensure protection of individuals' rights. Though the law specifies that the Board will be an independent body, unfortunately, the current Act has not specified the selection criteria for the members of the Board as well as the process. This will be articulated through subsequent rules. To strengthen the Board, various steps need to be taken: (1) a clear and transparent selection criteria should be established for the appointment of the DPBI members. It remains to be seen what kind of selection process and criteria will be established under the delegated legislation. (2) The selection process should prioritise candidates with adequate technical and judicial expertise to effectively handle the complex and dynamic nature of data protection issues. (3) In order to establish and maintain credibility and legitimacy, it is imperative that the DPBI should be adequately funded, staffed and equipped. (4) To further legitimise the independence and credibility of the DPBI for stakeholders, its decisions must also be upheld and implemented and not undermined by the government and the judiciary.

Some participants at the workshop were of the view that the institutional design and functioning of the DPBI echoes with that of an Ombudsman (with a limited and specified adjudicatory function) rather than an overarching regulator having a suite of powers relating to monitoring, awareness generation and standard-setting.⁶⁵ Some participants of the workshop observed that the current scheme may be a good starting point for India while it awaits the conceptualisation of a full-fledged regulator required for this ecosystem as we see in the EU and for other sectors such as banking and insurance in India.⁶⁶

Design Analysis of DPBI

Key features of a full-fledged regulator would require (1) a people-friendly grievance redressal mechanism (2) a trusted body that is independent from the executive and undertakes monitoring of the ecosystem, regulation making and stakeholder consultations (3) an adjudicator that has regional presence (4) regulator that actively identifies individual harms and collective privacy harms, investigates and undertakes suo moto actions and (5) establishment of an appellate authority. Currently, the proposed regulatory framework has envisaged the DPBI as a quasi judicial body and not as a regulator. Even as a quasi judicial body it is missing some of these key features

⁶³ K.S. Puttaswamy and Anr. vs. Union of India ((2017) 10 SCC 1; Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors (2019) 1 SCC 1

⁶⁴ The Personal Data Protection Bill, 2019, Lok Sabha (Bill No. 373 of 2019)' <http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf>

⁶⁵ The analogy emerged during the workshop while discussing the regulatory structures for the digital ecosystem. There is no official statement made by the government to this effect.

⁶⁶ Examples include the Banking Ombudsman Scheme and the Insurance and the Insurance Ombudsman are the quasi-judicial bodies for sectoral regulators.

(discussed below) which would be essential in ensuring effective access to justice:

1. *People-friendly grievance redressal mechanism* - The current formulation of the DPBI raises concerns around how this institution can be accessed by various stakeholder groups and whose interests are being represented and protected. The mechanism designed for grievance redressal under the DPBI has been criticised for disincentivising people from filing complaints to remedy privacy harms.⁶⁷ The onerous duties imposed on people,⁶⁸ the absence of compensation and the vague provisions through which the DPBI can close and conclude complaints, have been identified as the primary deterrents. Moreover, the Act places sui generis duties on people to access remedies such as obeying all the "applicable laws" of the land, refraining from submitting fraudulent complaints and abstaining from providing inaccurate details. This provision was inserted with the objective of preventing "misuse of rights" by people. The inclusion of a provision such as this is inadvisable as it runs counter to the objective of establishing accessible remedies for the population.

The current adjudicatory and justice model is pivoted on individual access to justice and relies on individually initiated complaints being brought before the DPBI. Taking into account the complexity of the domain and the collective nature of harms, the current model failed to grasp the opportunity of creating an optimal mechanism to identify harms by the DPBI and take action against erring data fiduciaries. This could have been achieved by empowering the DPBI to initiate suo-moto proceedings against entities instead of solely relying on individually initiated complaints. With no authority to monitor or investigate and address potential non-compliance matters, it seems that the DPBI may be unable to proactively identify and address significant harms. Another significant shortcoming is the lack of monitoring powers assigned to the DPBI to identify instances of collective harm.

The DPDP Act assigns certain adjudicatory powers to the DPBI, chiefly relating to taking prompt action in response to personal data breaches, investigating complaints, imposing penalties, and issuing directions such as requiring data fiduciaries to adopt urgent measures to remedy personal data breaches. However, the mandate to also protect the interests of people and prevent misuse of personal data have been removed. This power featured in the previous iterations of the law, proposing a regulator. Absence of a clear mandate for the DPBI on protecting the interests of people could dissuade people from approaching the DPBI and turn people to alternate forums which are riddled with pre-existing challenges. This could negatively affect people's right to access legitimate and effective justice delivery systems and may reinforce reliance on overburdened traditional

⁶⁷ Shashank Mohan, 'New Data Protection Law: It Cements the Power Imbalances in the Data Economy' (The Indian Express, 28 December 2022) <<https://indianexpress.com/article/opinion/columns/shashank-mohan-writes-new-data-protection-law-power-imbalances-economy-8348308/>> accessed 18 August 2023.

⁶⁸ Section 15, The Digital Personal Data Protection Act, 2023.

court systems leading to further delays in the resolution of cases. Moreover the judiciary may lack the technical skills and expertise required to deal with the complex technical issues relating to data protection.

2. *Building trust in an institution* - A requirement towards ensuring credibility and the reputation of an institution is the trust in the institution of the stakeholders who interact and engage with it. Trust ensures that individuals have the confidence in approaching the institution to seek the redressal of their grievances. The credibility and legitimacy of the DPBI depends on the following factors:

a) Building trust by securing independence - The effectiveness of a data protection regime is contingent not only upon the existence of a legal framework that safeguards privacy and liberty but also upon the establishment of an independent adjudicatory body.⁶⁹ With the government's mission of making the internet open, safe and trustworthy, having an executive appointed quasi-judicial body will not support this endeavour. The law empowers the executive to determine the strength and the composition of the board, the process of selection, terms and conditions of appointment and service, and removal of board members and other matters via its rule-making power. Hence, the independence of the DPBI has been considerably weakened in the DPDP Act with various stakeholders highlighting the same.

i) Lack of a Selection Committee - The lack of a Selection Committee to appoint members of the DPBI leads to further questions on its independence. This contradicts established judicial precedent, according to which the DPBI is a quasi judicial body⁷⁰ whose members must be appointed independently.⁷¹ International standards are also increasingly emphasising the need for national data protection regimes to ensure the independence of the data protection authorities. Under the GDPR, Article 52 creates a special provision to ensure the independence of the members of the supervisory authorities. It requires all DPAs in the EU to act with “complete independence” when carrying out their duties.

⁶⁹ David H Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* (University of North Carolina Press 1989).

⁷⁰ The Supreme Court has held in the case of *National Securities Depository Limited v. Securities and Exchange Board of India*[#] that the three requisites necessary to characterise the act of an administrative body as quasi-judicial are: (i) There must be legal authority; (ii) This authority must be to determine questions affecting the rights of subjects; and (iii) There must be a duty to act judicially. As per the provisions of Chapter 6 of the DPDP Act and the aforementioned test, the powers vested in the DPBI are quasi-judicial.

⁷¹ The Constitution Bench in *Supreme Court Advocates-on-Record Assn. v. Union of India*[#] held that there is a compulsory need for the exclusion of the Executive over quasi-judicial bodies discharging responsibilities akin to Courts. The absence of a procedure for the appointment of members of the DPBI and the exclusive power of the Executive to make appointments to the DPBI would be against the constitutional scheme inasmuch as they could be considered an encroachment by the executive over such quasi-judicial bodies. This would also violate the principles of separation of powers and independence of the judiciary.

- ii) Security of Tenure - The security of tenure of a member in an institution is essential to ensure credibility and independence in the functioning of the body. The DPDP Act 2023 provides for a two year tenure with eligibility for reappointment. However, the Supreme Court has stated that short-term appointments along with the provisions of re-appointment increases influence and control of the Executive.⁷²
3. *Building access by strengthening digital and regional presence* - The provision on creating a digital-by-design DPBI is welcomed as it focuses on ensuring ease of accessibility and affordability.⁷³ While the institutional design and working of this adjudicatory framework has not been detailed in the Act, it specifies following such a mechanism.⁷⁴ However, at this stage, we do not know the exact contours of the approach.
 4. If implemented seamlessly, this digital framework will encourage people to approach the DPBI with their complaints. However, the adoption may be concentrated to urban populations or certain socio-economic sections of society who have the awareness, the requisite skills sets and access to digital devices. This approach fails to recognise the challenges it may pose for individuals who have low levels of digital literacy or who reside in remote areas or those belonging to marginalised sections of society. The focus should be on building a hybrid model that has a regional physical presence and simultaneously builds the capacity and awareness of people and all stakeholders involved to begin online engagement.⁷⁵ Further, the effectiveness of the enforcement mechanism depends on building a decentralised model that has regional physical presence across India to avoid overburdening a central enforcement authority and to ensure that there is regional representation and access. A hybrid model (online and regional physical presence) which ensures regional presence of the DPBI may help in closing the justice gap which may arise if the DPBI is completely digital or centralised. Similarly, keeping in mind the linguistic and cultural diversity in India, such a regional presence would be important to ensure ease of access, reinforce trust and confidence in the body and provide equitable access and inclusivity.
 5. *Identifying harms* - The DPDP Act 2023 focuses on initiating individual complaints for personal data breaches and does not use the language of privacy/data harms. The

⁷² Rojer Mathew versus South Indian Bank Ltd & Ors., 2019 (369) ELT3 (S.C.)

⁷³ Joanne D'Cunha and others, 'Comments to MeitY on the Draft Digital Personal Data Protection Bill, 2022' <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>.

⁷⁴ Section 28, Digital Data Protection Act.

⁷⁵ Joanne D'Cunha and others 'Comments to MeitY on the Draft Digital Personal Data Protection Bill, 2022' <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/ccg-nlu-comments-to-meity-on-the-draft-digital-personal-data-protection-bill-2022-334.pdf>>

current adjudicatory system does not provide an opportunity to identify individual and collective privacy harms that may result from non-compliance. The harms that manifest subsequent to privacy and data protection violations are difficult to identify because of their amorphous nature. Similarly, while individual people are capable of bringing forward their individual complaints to the DPBI, there is currently no scope under the DPDP Act to assess and address individual or community level harms that may arise. The existing framework focuses on individual data breaches and rights and does not recognise the collective and communal experience of data and the relational dynamic between individual data rights and group data rights.⁷⁶ From an access to justice perspective, it is important to accommodate for protection of individual and collective privacy harms as well. The lack of acknowledgment makes it convenient to sidestep the issue in the guise of protecting individual rights. Further, an independent regulatory body could provide an unbiased assessment of the risks and vulnerabilities of the ecosystem, which could inform the development of more effective regulations.

Operationalizing an inclusive DPBI

In order to operationalise the DPBI, keeping in mind some of the concerns round data justice mentioned in the first section, some possible mechanisms that could be explored are:

a) *Digital Legal Aid Services*: Digital services can play a role in mediating access to legal solutions easily for marginalised groups by helping them bridge the justice gap through imparting legal awareness and building capacity. India has a host of such digital services which aim to expand legal services and awareness to all sections of society. The Department of Justice has launched a scheme to ensure expansion of its outreach initiatives such as Tele-Law, Pro Bono Legal Services (Nyaya Bandhu), and Legal Literacy and Legal Awareness programs. These initiatives and platforms can be leveraged and initiatives can be encouraged whereby individuals wanting to bring a claim before the DPBI receive support in filing complaints, receiving legal advice and connecting with lawyers and legal experts.

b) *Integration with Common Service Centres (CSCs)*: The Common Services Centre (CSC)⁷⁷ programme is an initiative by the Ministry of Electronics and IT (MeitY) in India, which aims to ensure easy access to digital services in rural and urban areas. CSCs act as service delivery points offering help in utility payments and accessing web-enabled e-governance services amongst other functions. To this end, it may be helpful to integrate CSCs and the DPBI, particularly on issues such as filing of complaints through the digital portal, providing internet safety resources and digital literacy programs educating people about tools and techniques to identify and prevent digital harms.

⁷⁶ Swati Punia and others (eds), *Emerging Trends in Data Governance* (National Law University Delhi Press 2022) <<https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/nlu-delhi-law-book-2022-ff-web-345.pdf>>.

⁷⁷ 'Common Service Center' <<https://cscindia.info/>> accessed 18 August 2023.

c) *Collaboration between DPBI and local informal justice systems*: It is clear that the concept of privacy can no longer be deemed to be a merely elitist concern. Surveys⁷⁸ conducted in the recent past have shown that while people from different socio-economic strata and age groups do not understand the harms and risks of the digital world, they do have expectations of privacy and place trust in the government to protect it.

Having data protection legislation and the establishment of an enforcement authority are promising foundational steps in ensuring access to data justice. However, access to justice cannot be limited to the mere presence of legislation and an adjudicatory authority. The implementation of the grievance redressal mechanism should prioritise exploring mechanisms which focus on creating last-mile access points to justice. The pre-existing network of infrastructure in remote and rural areas in the country could be leveraged to create more access point linkages with the DPBI. To also ensure effective collaboration with the DPBI, mechanisms should also focus on enhancing the capacity of these linkages to support the local community in accessing such avenues of justice. Lessons must be drawn from the effectiveness of some of the informal enforcement systems on fostering community engagement with problem solving, and building awareness of the digital harms and risks. Therefore, it may be essential to establish mechanisms for effective communication and collaboration between the DPBI and local-level access points, to ensure that vulnerable individuals have access to grievance redressal and other resources to address digital harms.

⁷⁸ 'Privacy on the Line: What Do Indians Think about Privacy & Data Protection?' (Dvara Research Blog, 16 November 2017) <<https://www.dvara.com/research/blog/2017/11/16/privacy-on-the-line-what-do-indians-think-about-privacy-data-protection/>> accessed 18 August 2023.

Conclusion

The core aim of our exercise was to closely discuss the conceptual notions underpinning data governance in the two jurisdictions as well as share experiences which could benefit the future development of regulatory measures. The discussions focussed on what 'data' means for different actors in the jurisdictions which is then legislatively understood. It also covered the issues of design of laws and institutions which lead to predictable enforcement failures. The common experiences across the jurisdictions indicate a sense of strategic de-emphasising of particular vulnerabilities due to geopolitical or economic interests which have an ultimate bearing on people and their access to justice in the data economy. We also saw that the emergence of plural perspectives in both jurisdictions, and the challenges between individual rights versus community rights, the private capture of public functions, the influence of big tech on regulation, and the increased commodification of data are struggles for powers that will play out in other arenas as well.

This policy paper captures some of these discussions and how they contributed to moving the needle forward on some of the critical issues revolving around data governance at this time. We argue that data is a flow and not a binary but legal regimes driven by economic interests aspire to undermine this aspect by ascribing an artificially definite structure. Rights have been co-opted by actors that wield power and influence such as the private sector. This challenge flows into the establishment and governance of institutions like Data Protection Authorities that either do not have adequate capacity or lack effective prioritisation of issues that are most important for data justice. Beyond institutional perimeters, communities have taken several steps to ascribe a sense of agency in their data. States must support such community-centric efforts rather than aspiring for a definitive legal and institutional framework that will never be entirely free of political and social hierarchies.

We elucidated these theoretical points through a concrete case study evaluating the pitfalls and opportunities for the data governance and data protection ecosystem in India through an evaluation of the political, economic and social realities of the prevailing legal ecosystem. While the formal enforcement ecosystem faces several challenges, strong communities and informal ecosystems may serve as the perfect complement.

Both India and the EU are at critical tipping points in how data and the surrounding ecosystem is perceived and regulated. We hope that the debates raised in this report causes policy-makers, the private sector and researchers to think more closely about the complex and contested pathways towards a genuine notion of data justice. This is essential as we aspire to build a world that is hinged not only on economic and security interests in data but also on genuine notions of empowerment.

