internet democracy project

DGN Policy Brief 03

November 2020

Data Governance Network
Anchored by IDFC Institute

Data sovereignty, of whom? Limits and suitability of sovereignty frameworks for data in India

Anja Kovacs and Nayantara Ranganathan

The concept of sovereignty has come to frame a number of data governance proposals by the Indian government. To understand the scope, import and consequences of these reassertions of sovereignty, it is, however, important to unpack the nature of the claims that have been put forward. In particular, to what extent do these promote the exercise of autonomy and choice by the Indian people? In order to benefit the people of India, assertions of sovereignty in the face of data colonialism will need to take into account that data is not merely a resource "out there", but increasingly functions as an extension of our bodies. As this analysis will show, current conceptualisations of data sovereignty fail to do so; for now, they therefore merely entail a transfer of power to domestic elites while doing little to return sovereignty to the people of India.

Introduction

Although there is no singular articulation of data sovereignty by the Indian government, shreds of it can be found in a number of legal and policy documents as well as in statements on data and new technologies made by government officials. In these formulations, sometimes technology and data are posited as means to secure existing sovereignty; at other times sovereignty is asserted over a new and strategically important kind of resource, that of data. And indeed, in a world in which control over data seems increasingly concentrated in a small number of hands, the concept of data sovereignty seems promising. But it is important to examine: what really is their potential impact? Who is constructed as the body containing this sovereignty? What are the accompanying policy prospects that current assertions of data sovereignty bring? And in particular, to what extent does this type of sovereignty further the exercise of autonomy and choice of the people?

In what follows, we first lay out the conceptual frameworks that animate our analysis, focusing on sovereignty and data, data colonialism, and feminist theories around the growing entanglements of data and bodies. This will elucidate the central claim of this policy brief: that the value of sovereignty frameworks in data governance crucially depends upon how we construct the nature of data. We then investigate how these different conceptual frameworks concretely infuse and animate sovereignty claims in a range of policy initiatives in India. We analyse regulations and proposals around data localisation, one of the central policies associated with the state assertion of data sovereignty in India. We also examine discourses around the economic value of data and ownership of data as crucial legal enablers of assertions of data sovereignty in their current form. Finally, we assess the light such theoretical frameworks can shed on the gains to be made by different stakeholders as a result of the data sovereignty claims put forward today.

1. Sovereignty: past, present and futures

Today's dominant conceptualisation of sovereignty as accruing to the state finds its origin in the Peace of Westphalia treaties, which recognised a new political order, organised around the co-existence of sovereign states as supposed equals. This sovereignty extended over lands, people and agents. In the early days of its proliferation, it was widely believed that the Internet was destabilising such state sovereignty, but in hindsight, this vision of the Internet was naive. As the uses of the network evolved and user bases expanded exponentially, legal concepts of property, expression, identity, movement, and context have not only retained their force, but have often been strengthened in new ways, precisely because of the

emergence of digital technology and its applications. These legal instruments are crucial means through which sovereignty in the digital age is operationalised, while sovereignty in turn is a key enabler of their enforcement.

Moreover, the link of sovereignty with territory continues to play a crucial role in its dominant articulations in the realm of data today, whether with regards to its external or internal aspects. The external is visible, for example, when changes to data flows are effected by obliging foreign firms dealing with Indians' data store that data within the country. The internal aspect concerns the legitimacy of the state to take decisions and ownership over the data of citizens. Both aspects contribute to the reconfiguration of power in the assertion of state sovereignty.

In addition, the concept of sovereignty has been adopted intentionally and incidentally by political technologists and activists working to reappropriate technologies. In these cases, it broadly denotes forms of independence, autonomy and control over digital infrastructures, technologies and contents (Couture and Toupin, 2019). Sovereignty in such cases is reclaimed and asserted as a claim to authority and the legitimate exercise of power to further self-determination, often in a direct challenge to the hegemonic power of the state and/or private actors.

Yet, caution is always advised against any uncritical adoption of sovereignty assertions as liberating. As the colonial powers used sovereignty to defend colonialism, there has been a deep entanglement between empire and modern assertions of sovereignty from the outset. Thus, our starting point in assessing any claims to sovereignty will need to be to ask: "who defines technological sovereignty and related concepts and for which purposes?" (Couture and Toupin, 2019: 5).

2. Sovereignty and data colonialism

This question gains particular importance in the Indian context, as the growing dominance of foreign big tech companies has led key Indian tech entrepreneurs and members of the government to cry foul about data colonisation (see e.g. PTI, 2018; Goenka et al., 2019).

Couldry and Mejias (2019) have argued that data colonialism is indeed a useful frame to understand modern forms of hegemony of big tech companies. They describe the slow emergence of a new form of capitalism, which is centred around the capitalisation of all aspects of human life, even the most intimate ones, and thus the normalisation of the commodification and exploitation of human beings, through data. As they explain, in the process of these shifts, a number of important parallels with historic colonialism emerge.

First, dominant discourses today frequently construct data that has actual or potential relevance to people as a resource that is simply "out there", up for grabs. As noted by Cohen (2018), this naturalises the collection of data in ways that have strong parallels with the construction by colonial powers of faraway, but clearly inhabited lands as *"terra nullius"* or "no man's land", thus legitimising their exploitation without legal intervention. In addition, Couldry and Meijas (2019) argue, such constructions of data hide from view that for such data to exist and for its capture to become a possibility, "the flow of everyday life must be reconfigured and represented in a form that enables its capture *as* data" (Cohen, 2018). This "redefinition of social relations so that dispossession came to seem natural" (Couldry and Meijas, 2019: 4) forms another important parallel with historic colonialism. To the extent that the state facilitates these practices, it becomes complicit in this dispossession.

Any challenge to data colonialism today can, then, only be effective to the extent that it challenges these underlying rationalities (Couldry and Meijas, 2019).

3. Bodies and data

What makes possible the dominant conceptual and metaphorical constructions of data with actual or potential relevance to people as a resource that is simply "out there"? We argue that the erasure of the connection between data and people's bodies is at the heart of this move. During historic colonialism, the construction of faraway lands

as *“terra nullius”* required the erasure of the bodies of the people who inhabited those lands – either physically, or by ignoring their traditions of occupancy and use. Today, it is the erasure of the close connections between data and our bodies that facilitates the construction of data as a resource.

Understandings of data as a resource “out there” find their origins in the discipline of cybernetics, in which these constructions of data have been dominant since at least the late 1940s. Data, such constructions maintain, is a layer of information that somehow penetrates everything, yet that can exist independently from the medium carrying it (Hayles, 1999). Thus, data or information has come to be thought of as both dematerialised and disembodied, something that can be easily and unproblematically transferred from one medium to the next. Moreover, this seemingly independent layer of information has been accorded enormous power: it has come to be seen as the ultimate truth-teller, somehow more accurate, more objective, more representative than what has ever come before, explaining to us how we, how things *really* are (Grinberg, 2017).

Much of today's dataveillance too, is informed by such understandings of data. Rather than targeting our bodies and selves in their totality, as in earlier eras, surveillance now takes the form of capturing purportedly disembodied data points about our bodies and their actions (Haggerty and Ericson, 2000). This also means that surveillance now is more dispersed, fragmented than was the case earlier. The purpose of surveillance today remains the same as before: to direct or govern our actions. But as context disappears from view and much now depends on which boxes we have been slotted into from the outset, pinpointing harms becomes more and more difficult (Haggerty and Ericson, 2000).

What disembodied constructions of data hide from sight, however, is that technology and data extraction are closely tied up in power relations – and this is particularly evident where data of actual or potential relevance to people is concerned. After all, if the bodies that generate data do not exist outside of the social world (as evidenced, e.g., by the fact that we do not treat all bodies equally even if we should), neither does data itself (boyd and Crawford, 2012). Processes of interpretation affect decisions about what to include and what to disregard at the design level, what to pay attention to and what to neglect during data collection and analysis. And even large data sets can be full of errors and gaps, amplifying the harms when the interpretation of the data happens without those doing the interpretation acknowledging their own biases or those that shape the data sample as such (O'Neil, 2016). Contrary to the cybernetic imaginary, context all too often does matter, and the impact of biases on the processes of datafication of our bodies and actions can have particularly severe consequences for those already vulnerable.

As even the most intimate aspects of our lives become subject to datafication, an even more fundamental shift is taking place, however: the distinction between our physical bodies and our virtual bodies is increasingly becoming irrelevant (van der Ploeg, 2012). For example, in India, reports have highlighted instances where people have not been able to access the rations they are legally entitled to because the authentication of their fingerprints, stored under India's unique ID or Aadhaar, which is mandatory to access rations, failed. Sometimes, this had starvation deaths as a result (Johari, 2018). When decisions based on our data bodies have such far-reaching consequences for our physical bodies, data clearly can no longer be considered simply a resource “out there”. Rather, it emerges as an extension of our bodies, even a part of it.

For the protection of our rights in the digital age, understanding this paradigmatic shift has profound implications. For example, when we understand that our data is an extension of our body, it becomes obvious that the harms of misuse of data might in some cases be better understood as, for instance, violations of bodily integrity than as data protection violations. If the sovereign state is to continue to safeguard the interests of the people who created it, it is thus essential that it takes these underlying realities regarding the nature of data into account.

4. Sovereignty through data localisation

Exemplifying the continued importance of territory, data localisation has emerged as one crucial, concrete mechanism under discussion to assert data sovereignty in India. Following Bailey and Parsheera (2018), this policy brief understands data localisation as "mandatory requirements of local storage of data", whether exclusively or in the form of mirror data copies, thus fundamentally steering, and altering, data flows.

In recent years, India already has put in place data localisation requirements in a number of sectoral policies. Moreover, although reports have indicated that these may be reconsidered (PTI, 2019), there have been various proposals for comprehensive data localisation over the past three years as well (sometimes with conditional exceptions), in addition to further sectoral requirements.

By reorganising data flows to gain greater control over them, broad-sweep data localisation proposals illustrate the profound reconfiguration of power that the assertion of state sovereignty in both its external and internal aspects can entail. In doing so, such proposals notably also recognise, even if implicitly, that the dividing line between our physical bodies and our virtual bodies is becoming irrelevant: after all, the aim of these policies generally is not merely to gain control over data as something that is "out there" but also as a means through which to control – or protect – the physical bodies of people, including by the state. The question that then emerges is: to what extent will this reterritorialization of their data benefit citizens and restore *their* autonomy?

The Puttaswamy Judgement of 2017 confirmed that sovereignty lies with the people, a part of which is vested in the different apparatuses of the state.[i] But data localisation proposals see the container of sovereignty somewhat differently. Thus, in a report on personal data protection in India, released in 2018 by the government-constituted Committee of Experts under the Chairmanship of Justice B.N. Srikrishna,[ii] the emphasis in discussions on sovereignty is on the nation-state, which will supposedly be able to enforce more effectively substantive obligations once data localisation is in place.

User interests do figure among the arguments presented in favour of data localisation in such discussions. For example, a common argument for sectoral data localisation is that certain kinds of data – such as health and finance data – require higher degrees of safeguards. But while this recognition is encouraging, important new challenges that have emerged in the digital age remain unacknowledged. Sensitive health data no longer lives only within hospital files, but includes data gathered by smart watches, browsing histories, searches about health conditions, etc. As elsewhere in the world, nothing in India's existing or proposed data governance policies acknowledges, let alone addresses, these realities.

In addition, the autonomy and choice of individuals are severely undermined if data localisation proposals become a reality. The selection of services available for use by Indians will shrink, and any discretion that Indians could have exercised to keep their data private and secure through choices about where to locate it will no longer be available.

The consequences of this loss of choice and autonomy are far-reaching. With their intense datafication, our bodies and their actions "become amenable to forms of analysis and categorisation in ways not possible before" – and this by a multitude of actors, all able to determine "who we are" and how we should be treated without us even having to be physically present (van der Ploeg, 2012: 177). Indeed, the erasure from view of the close connections between our bodies and our data obscures that measures like blanket data localisation are not merely about losing control over where to locate one's data; they are about the state, and select domestic private parties, gaining an unprecedented level of access and control over the bodies of Indian citizens, their actions and behaviour, without any escape possible.

While under the current legal regime, data localisation thus affects our freedom, agency and autonomy in unprecedented ways, such concerns are not reflected in discussions around data localisation today. Instead, much of the rhetoric around the objectives relating

to economic development and innovation in particular continues to support understandings of data as a resource (see e.g. Bailey and Parsheera, 2018). Moreover, the drive towards data localisation by state institutions is further supported by important sections of India's tech-based industry (Mandavia, 2019), some of which, such as Reliance Jio, have appropriated the frame of data colonialism to promote such proposals in the service of their own interests. As data colonialism today need not only be directed towards those outside of a state's territorial boundaries, the close entanglements, and revolving door, between government and key industry players with a stake in the data localisation debate deserve to be watched closely. For now, data localisation in India seems to merely entail a transfer of power to domestic elites, while doing relatively little to return sovereignty to the people.

5. Enabling the construction of data as a resource

As noted above, in the production of the claim of Indian data sovereignty, constructions of data as a resource continue to be dominant. For this resource extraction that is at the heart of surveillance capitalism to have become possible, enabling legal constructs had to be created (Cohen, 2018). In Indian law and policy proposals, two tools are of particular importance: a strong emphasis on the economic value of data at the expense of other concerns, and the particular resolution of questions of ownership that the Indian government proposes. Both contribute to the erasure of our bodies from the data governance discourse.

5.1. The economic value of data

Data sovereignty claims in India have constructed data as a primarily economic resource to be used in the service of economic enrichment of the country and the consolidation of Indian companies' market share. While other concerns may be paid lip service to, in practice they are subordinated to these financial considerations. Assertions of data sovereignty have emerged as a central means to lay claim over the data of Indians and its value.

If data is being generated in ever-larger volumes, this is is not a naturally occurring phenomenon or inevitable in the development of technology, but a result of a market where there is both demand for more data and a promise of development from this data. However, in Indian policy documents and proposals, data being *out there* and available in ever-increasing volumes, as well as it being a productive factor in the economy, are presented as a given. Business models to monetise this data are then framed not only as desirable, but imperative.

For example, despite the wealth of literature criticising the lack of meaningful consent to the collection, processing and storage of our data, the Economic Survey 2018-2019, published by the Ministry of Finance, Government of India,[iii] constructs personal data as being consensually shared by people “of their own accord” (79). This ignores that the architecture of our daily lives has been intensely transformed to facilitate and encourage the production of data at every step. The Economic Survey 2018-2019 further makes it appear as if capital to process data, and the technical skills surrounding it, are factors that come into being post the fact of generation of data (79), rather than being drivers of the generation itself.

Similarly, the draft National e-Commerce Policy,[iv] released in February 2019, highlights the monetisation of data as a possible key enabler and critical determinant of India's growth and economic development (11). However, it fails to address criticisms that this business model, while thriving in the digital economy, has also reduced space for traditional business models, and has increasingly come to be seen as damaging to the use of the Internet.

That the generation of data in increasing volumes is neither inevitable nor natural, and that its commercialisation is not necessarily desirable, is, thus, overlooked. After the construction of data as raw material available for the obvious purpose of economic enrichment, the draft National e-Commerce Policy, in fact, actively encourages the problematic dominant business models that are built around extraction in order to shape behavioural modifications. The draft Policy

approvingly states: "companies with maximum access to data about consumers stand to make windfall profits from leveraging this through targeted advertising and product development" (12). Elsewhere, it uncritically lauds big data and artificial intelligence. The draft Policy thus completely ignores that such practices are at the heart of what Zuboff (2019) has labelled "surveillance capitalism", a form of capitalism in which companies are effectively making profits by taking bets on people's future behaviour. Such practices have increasingly been highlighted as extremely problematic (see e.g. Zuboff, 2019).

5.2. Ownership of data and sovereignty

Notions of ownership of data and property also animate policy debates around data in India to a significant extent, both in government documents such as the draft National e-Commerce Policy and through titans of industry, such as Mukesh Ambani (PTI, 2018). However, the paradigm of ownership in the context of data, too, does little to challenge the rationalities that underlie data colonialism, while continuing the myth that data is always at a remove from our bodies.

Like consent, the ownership paradigm only provides limited control if the parameters of the market in which it has to operate are already established. In particular, within this market, much of our data has value not on its own, but when combined with data points from a large number of other people. Moreover, based on the analysis of such large, aggregated data sets, inferences may be made about us even if our own data is not included in the original data set (Haggerty and Ericson, 2000; van der Ploeg, 2012). Having ownership over our data will not stop this from happening.

Bringing bodies back into the debate can further elucidate what is at stake here. In democratic societies, questions of human dignity and bodily integrity have never been reduced to questions of "ownership". Thus, Indian laws make it impossible to sell yourself into slavery even if you want to. While private property might be protected, ultimately the values of freedom, agency and dignity gain primacy. In a similar vein, protecting our freedom, agency and dignity in the digital age requires that our data is not merely reduced to a resource that we can trade in a deeply asymmetrical market in which we hardly have any power.

Questions of ownership of data do not only figure in debates about individual users. In its 2018 report,[v] the Srikrishna Committee articulated for the first time a category of data called "community data". Deploying "community" in a very loose manner, the Committee distinguishes community data from big data sets depending on the degree of involvement of "the larger community" in building the dataset. Thus, for the Committee, data gathered by products of private companies like Google Maps constitute an example of community data.

Considering community data "information that is valuable owing to inputs from the community" (24), the Committee notes that community data relates to a "group dimension of privacy", and lays down a vision for higher protection of this data, including by providing for class action remedies where the harm is social and systemic. At the same time, however, the Committee creates a space of dispersed ownership by saying that ownership of community data is, in fact, difficult to ascertain.

In other technology policy documents, such as the draft National e-Commerce Policy, the concept of community or the commons is, in fact, used strategically in the realm of the digital to create a vacuum of ownership, which is then followed by such ownership being asserted by the government. As the draft Policy then continues to argue that rights are "permitted" over this resource that the government holds in trust, it effectively makes these rights secondary to the government's priorities for the data (14, 15).

Moreover, while both "community data" and "public interest" are central concepts in the draft National e-Commerce Policy, with "public interest" used as a justification to allow for the *commercial* exploitation of data by start-ups and firms (17), they are not defined. Without definitions, or an understanding of how to grapple with competing interests of different communities

and with the fact that data can simultaneously be personal data as well as community data, the category of “community data” only serves to create a class of data over which individual claims for protection can be weakened.

The draft Policy, thus, radically differs both ideologically and practically from the examples of reclaiming control over data that it lists, such as the Maori Data Sovereignty Network and Project Decode in Barcelona. The starting point for indigenous data sovereignty is an understanding of who comprises the community. Moreover, the framework of community data has emerged from demands by these communities for control over their own data in the service of self-determination and self-governance. This includes an understanding that the usefulness of data depends on a range of factors, including the extent to which it reflects “tribal needs, priorities, and self-conceptions” (Rainie et al., 2017). Such baseline understandings are missing in the Indian government's proposal.

Further, these proposals disregard that the commons has never been without its problems in the Indian context, as elsewhere. From public space to wells of drinking water, the commons are spaces where there is exclusion on the basis of caste, and to an extent gender and other barriers (Nath, 2019). Even where there are no clear lines of discrimination, there are competing interests over the commons.

Without surfacing these complexities, “community data” becomes a category where the ownership is somewhat dispersed, the outline of who forms a community and how decisions over it can be taken is absent, and room is essentially created for other types of claims to be asserted: by the state and by the private sector, as well as possibly by other powerful actors within this “community”. Thus, the concept of community data seems to be foregrounded in India to make available ever more data in the service of the “national interest” and India's aspirations for global dominance, rather than the freedom and autonomy of India's diverse communities.

Conclusion

As we have illustrated, data sovereignty in India is a vision created and asserted by arms of the government with strong support from select sections of India's tech industry, and imagines the state as the vessel of such sovereignty. It rests on the portrayal of data as a resource, an emphasis on its economic value at the expense of other considerations, and the centrality of the notion of ownership (rather than dignity, freedom, and/or integrity). While individual privacy and autonomy of citizens do find mention in policy documents envisioning data sovereignty, they are not fleshed out, or are seen as secondary to larger collective agendas, such as economic enrichment as defined by the state and powerful private actors.

As a consequence, assertions of data sovereignty in India currently are largely limited to rallying against foreign entities gathering the data of Indians, while stewarding and encouraging the extraction of the same data by Indian entities. This enables the Indian state and domestic private actors to gain far-reaching control over the data of Indian citizens, and in the process, over their bodies, actions and lives. Moreover, because of the erasure of bodies from data governance discourses, this can happen without the substantial protections and accountability measures that typically attached to such decisions and activities in the pre-digital age. Strong rights protections that centre the link between Indians' data and their bodies and selfhood are not emerging. The questioning of data colonialism's underlying rationalities in law and policy that is essential to further the rights of Indian citizens in a substantive manner, and to thus protect their bodies and selves, remains absent as well.

All this has far-reaching consequences for the Indian people who transferred part of their sovereignty to constitute the Indian state: rather than furthering their autonomy, freedom and dignity in the digital age, it substantially undermines it. For the people, if not the state, data sovereignty, for now, continues to remain a dream.

Notes

i. Writ Petition (Civil) No. 494 of 2012.

ii. Available at https://meity.gov.in/writereaddata/files/

iii. Available at https://www.indiabudget.gov.in/economicsurvey/.

iv. Available at
https://dipp.gov.in/sites/default/files/DraftNational_ecommerce_Policy_23February2019.pdf.

v. Available at https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

References

Bailey, R. & Parsheera, S. (2018, 31 October). Data Localisation in India: Questioning the Means and Ends. New Delhi, National Institute of Public Finance and Policy, Working Paper No. 242. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356617

boyd, D. & Crawford, K. (2012). Critical Questions for Big Data. *Information, Communication and Society,* 15(5): 662–679. https://doi.org/10.1080/1369118X.2012.678878

Cohen, J. E. (2018). The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy. *Philosophy and Technology,* 31(2): 213–233. http://dx.doi.org/10.1007/s13347-017-0258-2

Couldry, N. & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media,* 20(4): 336–349. https://doi.org/10.1177/1527476418796632

Couture, S. & Toupin, S. (2019). What Does the Notion of 'Sovereignty' Mean When Referring to the Digital? *New Media and Society,* 21(10): 2305–2322. https://doi.org/10.1177/1461444819865984

Goenka, V., Patil, V. M., Shekatkar, D. B., Khandare, V., Bhatia, V., Ranade, J., & Panchal, B. (2019). *Data Sovereignty: The Pursuit of Supremacy.* Delhi: Penman Books.

Grinberg, Y. (2017). The Emperor's New Data Clothes: Implications of 'Nudity' as a Racialised and Gendered Metaphor in Discourse on Personal Digital Data. In J. Daniels, K. Gregory, & T. McMillan Cottom (eds.), *Digital Bodies.* Bristol: Policy Press.

Haggerty, K. D. & Ericson R. V. (2000). The Surveillant Assemblage. *British Journal of Sociology,* 51(4): 605–622. https://doi.org/10.1080/00071310020015280

Hayles, K. N. (1999). *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics.* Chicago: University of Chicago Press.

Johari, A. (2018, 3 February). Yet Another Aadhaar-linked Death? Denied Rations for 4 Months, Jharkhand Woman Dies of Hunger. *Scroll.* https://scroll.in/article/867352/yet-another-aadhaar%20linked-death-jharkhand-woman-dies-of-hunger-after-denial-of-rations

Mandavia, M. (2019, 22 February). How Desi Tech Lobby Is Giving Silicon Valley Giants a Run for Their Money. *Economic Times.* https://economictimes.indiatimes.com/tech/internet/how-desi-tech-lobby-is-giving-silicon-valley-giants-a-run-for-its-money/articleshow/68102813.cms

Nath, A. (2019, 22 August). Tamil Nadu: Funeral Procession Blocked, Dalits Airdrop Body for Cremation. *India Today.* https://www.indiatoday.in/india/story/dalit-man-funeral-processiondenied-in-vellore-community-says-not-the-first-time-1590160-2019-08-22

PTI (2019, 23 July). Personal Data Protection Bill: IT Ministry May Back Storage Curbs for Critical, Sensitive Data. *The Hindu.* https://www.thehindubusinessline.com/info-tech/personal-data-protection-bill-it-ministry-may-back-storage-curbs-for-critical-sensitive-data/article28682941.ece

PTI (2018, 19 December). Mukesh Ambani Says 'Data Colonisation' as Bad as Physical Colonisation. *Economic Times.* https://economictimes.indiatimes.com/news/company/corporate-trends/mukesh-ambani-says-data-colonisation-as-bad-as-physical-colonisation/articleshow/67164810.cms?from=mdr

Rainie, S. C., Schultz, J. L., Briggs, E., Riggs, P. & Palmanteer-Holder, N. L. (2017). Data as a Strategic Resource: Self-determination, Governance, and the Data Challenge for Indigenous Nations in the United States. *The International Indigenous Policy Journal,* 8(2). https://ir.lib.uwo.ca/iipj/vol8/iss2/1/

van der Ploeg, I. (2012). The Body as Data in the Age of Information. In K. Ball, K. Haggerty and D. Lyon (eds.), *Routledge Handbook of Surveillance Studies.* New York: Routledge.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* New York: Public Affairs.

Data Governance Network

The Data Governance Network is developing a multi-disciplinary community of researchers tackling India's next policy frontiers: data-enabled policymaking and the digital economy. At DGN, we work to cultivate and communicate research stemming from diverse viewpoints on market regulation, information privacy and digital rights. Our hope is to generate balanced and networked perspectives on data governance — thereby helping governments make smart policy choices which advance the empowerment and protection of individuals in today's data-rich environment.

About Us

The Internet Democracy Project works towards realising feminist visions of the digital in society, by exploring and addressing power imbalances in the areas of norms, governance and infrastructure in India and beyond.

Acknowledgements

This policy brief draws on a paper with the same title by Anja Kovacs and Nayantara Ranganathan. . The policy brief was prepared by Anja Kovacs, with support from Shraddha Mahilkar and Tanisha Ranjit.

IDFC Institute
3rd Floor, Makhija Chambers, 196 Turner Road,
Bandra(W), Mumbai 400050

/idfcinstitute @idfcinstitute /IDFCInstitute