Human Security in a Datafying South Asia: Approaching Data Protection

Preeti Raghunath

Abstract
In an increasing datafying world, protection of data created and generated as a result of everyday interactions assumes imperativeness. Last year, Europe adopted the General Data Protection Rules (GDPR), which has yet to be subject to substantial reviews to check for inconsistencies and possible blind-spots. Similarly, other national (like India and Brazil) and regional juridical bodies seek to work out frameworks that address data protection. This paper looks at some possible ways to think about Data Protection legislations and practices in South Asia. By alluding to ideas of data justice (Taylor, 2017; Dencik, Arne & Cable, 2016) and underscoring the idea of 'multiplicity' of data regimes, this essay paper draws on the idea of human security (King & Murray, 2001) as central to thinking about data protection legalities. This is does, by placing the protection of the essence, proprietary and otherwise, of the human, at the centre of this legal exercise of formulating data protection legislations, to uphold data democracy.

Introduction

In May 2018, the European Union adopted the General Data Protection Regulation (GDPR) as a legal measure to harmonise the many nuances of data-centric practices and their governance. Along similar lines, countries of the Association for South East Asian Nations (ASEAN) have enacted and implemented legislations that serve the data protection mandate. India, last year, put out a white paper on data protection calling for comments and feedback from various stakeholders, many of whom responded. It is anticipated that the new government that has come into power will be tabling the data protection-related legislations in the country's Parliament for law-making.

The modern regulation of practices around data like collection, storing, processing, and utilizing, is currently gaining prominence due to increasing focus on data-driven economies and industry. Growing datafication of work and society is being witnessed today, with data gaining immense importance, being remarked to be as important as oil. This paper

looks at ways of thinking about data protection legislations, especially from the vantage point of South Asia. Do the regulatory structures and experiences posit different priorities and problems for the region, in comparison to the rest of the world? Does a non-Western viewpoint to data protection exist? What would a critical data studies approach to the study of data protection legislation draw on? Finally, how does implicating the human in a data-centric discourse change perspectives? These are some of the questions that this short paper concerns itself with, and tries to theoretically address. The first part of the paper tries to understand the legislation, implications in terms of sovereignty, and jurisdiction of data protection regulations. The second part seeks to present the landscape of data protection legalities in South Asia. The third part of the paper provides the mediating ecosystem in South Asia. The fourth and final part of the paper explores the fertile terrain of critical data studies, registering analytic notes on data protection legalities from this vantage point.

I. Legalese: Understanding Legislation, Sovereignty, and Jurisdiction

This author isn't a lawyer and does not hold a law degree, and deems it imperative to demystify legalese and translate it to commonly understood parlance. Laws and regulations are often very complex and even ambiguous, especially when they encompass a range of experiences akin to what the GDPR seeks to cover, to account for those plural experiences. Often, one country's experiences may not stack up against another country's. Similarly, the realities of one sector may not mirror itself in another. Therefore, when it comes to generic data protection legislation, understanding the interrelated triad of law – the legislation itself, the idea of sovereignty that the law implicates, and the regional and distributive focus of the jurisdiction in terms of legislating using the law -- become important.

The Legislation

Legislations on data protection, more often than not, seek to outline the boundaries for fair use of data, in order to protect the privacy and claim over personal records and activities, of individuals and entities. The subject of the legislation is an important aspect to consider. Who or what should the data subject be? Couldry and Yu (2018) contend that the GDPR is grounded in human rights, and poses a big challenge to datafication, especially in the wake of recent misgivings like the Cambridge Analytica fiasco. However, they point that the rights approach is limited when faced with claims of data being collected for public interest. The challenge the very idea that data *should* be collected, as if it is a natural process. They underscore the constructed nature of data collection, and seek to deconstruct the

assumptions behind the inescapability from datafication, or Big Data Exceptionalism (for which they draw on Nissenbaum (2017)). Couldry and Mejias (2019) elucidate the idea of data colonialism, as a form of appropriation and extraction, instead of solely looking at it in traditional Marxist terms, of making data as labour.

The dichotomy of the public and the private is at the heart of data protection legislations. However, the idea of intersubjectivity and the dialectics of the interaction between the private and the public can challenge this dichotomous, sealed categorising of the very human experiences of being and becoming, in these times of hyperconnectedness. Discourses around the GDPR speak of the 'data subject' to be the human; however, the larger contextual and ecological frame gains importance, in order to make sense of the human subject, including but not inclusive of the impinging structures of dataveillance and control. What, then, constitutes the protection of human data?

Sovereignty

Christopher Allen presents the idea of 'self-sovereign identity' (2016), as a way of defining individual identity today, beyond the yolk of companies or the state or other conferrers of identity. He speaks of an innate, inalienable sense of identity beyond what is prescribed and conferred upon individuals, categorizing and branding them as citizens as against migrants, as voters or employees or as individuals eligible for social security. Allen draws up four stages of the evolution of identities in the digital sphere, and develops his concept of 'self-sovereign identity' as closest and in sync with the natural, inalienable sense of identity. This means that the individual user is in full control of their data, and holds sovereign authority over it without ceding to organisations that manage data for the user. Tobin and Reed (2017) of the Sovrin Foundation draw on Allen to suggest that self-sovereignty can be imagined as "a digital record or container of identity transactions that you control" (2017: 8). The authors go on to talk of self-sovereignty as an opening in the silo-centric view of data capture and veillance by organisations of all kinds. Moving beyond silos, self-sovereignty allows for fluidity, allowing for control in breaking patterns of data ownership by corporations and governments. Self-sovereignty is also marked by portability --- the ability of data subjects, and owners, if you will, to transfer and manouvre their data according to their desire. This is another manifestation of the fluidity associated with self-sovereignty, in ways that go beyond turgid stratification of data points.

It seems that the GDPR allows for the rights of humans in the EU to be protected in text, in the face of increasing datafication, by enshrining the following:

- Right of access to data profiling
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object

It remains to be seen how the claims over these rights are mandated, complaints mitigated, and how the GDPR is operationalized on the rights front. While the repose of sovereignty and related rights has been elucidated, the extent and expanse of the data protection laws requires emphasis, and is outlined below.

Jurisdiction

The third of the triad when it comes to data protection legislation is the jurisdiction of the law as it is implemented. Jurisdiction would cover the geographical reach and expanse, the depth and extent to which the law implies, and the components of such law.

In terms of the territoriality, data protection law, in consonance with the ways of the internet does not obey national boundaries. The GDPR illustrates the manner in which territoriality is not limited to businesses housed in the EU, but encompasses businesses that are operational in the EU, and indulge in data processing and storage of any kind, in the EU, or engage in data related to the citizens of EU nations. The referent object, clearly, are the individual citizens of EU. The Internet Society, in its update on May 25, 2018, suggested that with the GDPR, "Europe seeks to position itself as a de facto global regulator for privacy" (ISOC, 2018). The scope of the law in terms of the depth and its components are yet to be assessed and beg experience. How would non-digital interfacing between EU citizens and data collectors be measured and compliance ensured under the GDPR? How would non-citizens figure under the purview of the law?

Data Localisation is another related facet of jurisdiction of data protection laws, wherein the data that is collected, processed or stored is to be done within the territorial bounds of a country, in order to minimize threat of data dissipation, theft, or malpractice. For instance, IBM in India recently suggested that they would like to reverse the ownership and

localization pattern, against commonly understood strategies. A spokesperson suggested that the "users" would be the owners of data, but the data itself must flow freely. In terms of data processing, the spokesperson seemed to suggest that the company would take Artificial Intelligence to the users, and not vice versa. Evidently, the region in its broader meaning, emerges as the mediating space/mechanism, as it houses determining factors that affect the implementation of data protection. The next section examines the regional lens in closer detail.

II. Approaching Data Protection Legislation: A View from South Asia

Is there a regional view to data protection? A Europe-wide data protection regulation certainly seems to provide an answer, though one needs to examine if the EU emerges as an exception instead of the norm. This section of the paper seeks to probe into this question, looking at the region as a lens to study the theory of data protection legislation. Geographic markers like the region bring with them specificities that emerge as contributing factors to any experience of legalities. The particularities of histories, culture, physical topography, societal setup and economic environments characterise such an experience of the legal. When it comes to South Asia, one may argue for a "South Asianness" that comes to colour legal experiences. A common colonial past have granted the countries that make up the region, similar legal systems. Along the same lines, interconnectedness of society, language, religions, tropical climactic conditions, and economic conditions are attributes of the South Asian region.

India, the biggest South Asian nation recently put out a draft paper outlining the legalities of the data protection regulations. Calling for comments and responses, the Telecom Regulatory Authority of India (TRAI) put out the paper for consultation with various stakeholders to a data protection law. Numerous organisations, legal firms and independent lawyers sent in their feedback and ideas. Last year, India's communication policy landscape saw the pronouncement of Justice Puttaswamy, in the, upholding the Right to Privacy. The country is yet to see any articulation of a data protection authority who would uphold the legalities around data protection, nor is there a law as yet.

Graham Greenleaf (2013) argues, in an older paper, that Nepal's Right to information (RTI) laws that pertain to public bodies, have important clauses and implications for privacy in the Himalayan country. He examines the RTI legislation, the Interim Constitution of 2007 (prevalent at

the time of his writing the paper), the fact that Nepal is a signatory to the International Covenant on Civil and Political Rights (ICCPR), among other legal provisions. He suggests that Nepal is a frontrunner in South Asia, when it comes to privacy-related clauses. He writes:

> Nepal's RTI Act has almost all of the features that could be expected in a data privacy Act for the public sector in relation to personal data, such as are found in the OECD Guidelines: right of access; right of correction; protections against access by others; restrictions on use and disclosure by government agencies; restrictions on additional uses by third parties when they do obtain access; 'openness' of government practices concerning personal data; both offences and compensation provisions for breaches; an independent authority to investigate complaints and resolve disputes; and a right of appeal to the courts.

In an updated article, Greenleaf (2017) draws on the Constitution of 2015, to highlight Articles 28 and 47 that underscore privacy. He foresees the creation of a data protection law in the coming years, in Nepal. The country has since seen the passage of a privacy law, the Privacy Act of September 2018, which governs the storage of private information by public authorities.

Bangladesh had seen some articulations in the form of editorial pieces in newspapers, calling for data protection laws in the country. The country saw the enactment of the Digital Security Act of 2018, in October last year. Article 26 of the Act underscores consent and authorization by the individual. In addition, the constitution of Bangladesh underlines the sanctity of home, and release from undue government scrutiny. Similarly, Pakistan put out a Draft Personal Data Protection Bill in 2018, by the Ministry of Information Technology and Telecommunication (MOITT). The Bill also focuses on consent, and speaks of a new enforcement body, the National Commission for Personal Data Protection (NCPDP), to be established. In addition, the country's cybercrime policy focuses on cyber offences and related punishments. Afghanistan does not have a data protection law in place either.

The island-nation of Sri Lanka does not have a data protection law, but recent reports suggest the formulation of the Data Protection Bill anytime soon. There are provisions in the country's Constitution that pertain to the fundamental rights of individuals. De Soyza contends that Article 17 with Article 126 (1) could be as the safeguarding of individual rights against administrative or executive action. Similarly, Article 14A of the 19th Amendment to the Constitution is also seen as touching upon the idea of

privacy. The Information and Communication Technology Act of 2003 is an important Act, and the government suggests that it "is pursuing a policy based on the adoption of a Data Protection Code of Practice, encompassing the private sector, with the possibility of the code being placed on a statutory footing through regulations issued under the Information and Communication Technology Act of 2003. As such, this approach can be seen as self- or co-regulatory approach".

The Bhutan government's E-Government Master Plan features the mention of data protection a few times in a futuristic vein, as "emerging issues", and in proposed plans of action. Greenleaf (2017) suggests that Bhutan Information Communications and Media Bill 2016 provides for data privacy clauses, and he cites Chapters 17 and 21 of the Bill providing a comprehensive data privacy code, besides providing directions on how processed or collected data must be treated if it becomes obsolete, etc. In the Maldives as well, no data protection laws exist at this moment. The country put out a tender last year for the Translation of Privacy and Personal Data Protection Act (ibid.)

This section provided an overview of the legal framework on data protection, where they exist, in South Asia. While these frameworks may define the instrumental legal aspect of data protection, the human experiences are mediated by the larger structural and systemic attributes. The next section looks at these aspects, in order to arrive at an integrated overview of the state of affairs when it comes to data protection in South Asia.

III. Mediating Ecosystem: Some features

The South Asian region, replete with the above legal setups with respect to data protection, has some unifying features that together emerge as an ecosystem, mediating laws and experiences of such legalities. This section explores the idea of the region as a mediator, in order to understand the stake that South Asia has in data protection legalisation.

Access: Data protection, and indeed data itself, is the result of a collection of practices that generate recognizable imprints. During such a process, ***access*** becomes integral to the study of data and its protection. Access, in this case, can be defined in varied ways, ranging from access to information, access to infrastructure, and access to conducive environments. The World Bank describes South Asia as the fastest growing region in the world.

However, the region continues to experience vast disparities in terms of access, especially with digital access rates being very low. Given such a scenario, human access to information and technologies that could help repudiate corporate and private or even national governments' claims over data are not widespread. Access to information and technology that allows for redressal against data capture clearly emerges as an integral mediating aspect of the rights paradigm. For instance, there was some news about a data breach with India's national biometric identity system, the Aadhaar, which allegedly compromised the biometric details of those who have enlisted with the identity system. In response, the government suggested that access to the database was limited, and that there was no cause for worry.

Critical Information Infrastructure: Critical Information Infrastructure (CII) refers to infrastructure that are marked as critical to information economies. Determining what constitutes or comes under a country's CII is fraught with ambiguity, as the parameters for deciding which assets could be termed CII is often a tedious exercise. A country's CII is a determinant in the security of important data and information. The definition and identification of CII in South Asia is at a nascent stage currently. Infrastructure, especially of this kind, accentuate or inhibit the protection of human data, only stressing the need for more of the former variety. Often times, the focus on national security that is intricately intertwined with CII, their identification and maintenance obfuscate human security, at the other side of the spectrum. As a substantive data collection point, CII are vulnerable to data breaches and theft, exposing not just national security vulnerabilities, but also risking the lives of the humans that make up a nation.

Business environments: The larger business environments in South Asia have been characterized as modernizing and welcoming, according to the World Bank's *Doing Business 2015* report. The larger business environment acts as a catalyst in providing for facilities and/or obscuring the lives of many individuals, depending on how "good" the business is. The critical political economy reading of data would help unravel the interdependence of businesses that process, control or store data on the one hand, and the customers, employees, and other individuals on the other.

Larger socio-legal environments – privacy in itself: Another key layer that emerges as an important determinant is the state of privacy itself in the region. This is intricately intertwined with the quality of democracy, the socio-cultural setup, and the larger legal system in place in the region. In

South Asia, two points of views are oft repeated --- (a) that the South Asian culture is bereft of keenness on privacy; and that (b) the poor don't usually care for privacy and that it is an elitist concern. The cultural and class arguments on privacy have also faced rebuttals with work on religious grounding of privacy, and legislations like the Puttaswamy pronouncement that provide an equal footing for all citizens in their claim to privacy.

A regional view of data protection legalities, despite them being at a nascent stage in South Asia, is perhaps possible owing to the numerous commonalities in terms of the above descriptions, despite nation-bound differences as described earlier on. Such a regional view would be negated if national contexts offer vastly different circumstances. However, it may be noted that the above description falls short of regional legal sanctity with the SAARC being critiqued for almost withering away, unlike its South-East Asian counterpart, ASEAN, which has seen some development on this front.

South Asia's experience with data protection is evidently at a nascent stage. Intermediary factors like disparities in access and infrastructure on the one hand, an only growing business climate, and a somewhat closed up socio-legal environment providing for a mixed experience with data protection, that is markedly different from the Western experience.

IV. Registering Analytic Notes: Drawing on Critical Data Studies

In interrogating the intersections of the region and data protection, calls for Critical Data Studies to take cognizance of the spatial turn in data and contextualize it (Dalton and Thatcher, 2014; Taylor, 2015) gain imperativeness. Dalton, Taylor and Thatcher (2016), in particular, suggest that critical data studies (CDS) allows to understand the formation of the "subject", and makes space to understand the individual's actions, their subjectivities, reactions and resistances to a data regime. CDS goes beyond concerns of businesses and private players and their stakes in the business of data and data protection, to privilege the individual "subject". The human element is an integral aspect of interrogating structures of algorithmic assemblages, to reiterate and bring back the focus on the individual who generates data through everyday interactions and activities.

Data Justice and Data Protection: Predictability versus Precarity

One of the cornerstones of a just data protection law is also to provide for data justice, in general. This would translate into meaning that a just data protection law ought to provide the individual, freedom from undue

intrusion and surveillance. While evangelists of algorithmic lives promise neat predictability and enhanced quality of life and well-being, the precarity of life that is hinted at, by dataveillance (Dencik, Arne & Cable, 2016) and hyper-security networks conjures up a Frankenstein-like scenario.

While privacy is often the go-to concept in order to justify data protection, informational privacy marks up dangers of what could turn out to be information monopoly, with only those with access to information from the top leading fully informed lives. Algorithmic profiling only plays into the hands of the information elites, reinforcing their claim to data as well as privacy. Informational privacy spoken from the ground up certainly has potential, if the power in deciding the contours of this privacy rests with the individuals on ground. How does one understand the case of non-citizens, especially in the case of the migrant crisis in Europe? Would they be covered by the GDPR? Clearly, unless the response to datafication is not rooted in the human (which goes beyond the contours of defining an individual), and in contexts of data placement and operation, precarity is the order of our datafied lives.

Newman (2015), in particular, talks about big data being an issue of economic justice, and not just privacy, especially in newly forming data economies. Newman suggests that algorithmic and behavioural profiling that occur on free-to-use platforms are exploitative and generate data at the cost of free labour disguised as entertainment. Similarly, algorithmic profiling and condensation of data into newer forms of recognizable imprints bring in the disciplinary element (Johnson, 2014) of data injustice (Taylor, 2017). When a legal instrument like a data protection law is enacted, it ought to protect the individual from the ramifications of such cases of economic injustice and disciplinary manouvres by the information elite and controllers of data.

Multiplicity of Data Regimes: A Thousand Splendid Suns

The idea of data regimes draws on institutional theory, to underscore the integrated functioning of data, actors in the data space, norms, and interests, together to form structures of power and governance. Data regimes are whirlpools of power, since they structure interactions and the security apparatus around them. Private firms and conglomerates are often part of a data regime, processing and handling data, controlling output and creating and structuring lives and bodies of data.

In order for data protection to be a worthwhile endeavor aimed at achieving liberty and empowering the individual, a closed network of data regimes need to be broken down to give way to an open organisation of multiple data regimes that liberates individuals, citizens, customers, and other "owners" of data. By breaking down rigid structures of power, and allowing for multiple legacies and owners of data, numerous manifestations and utilisations of data are rendered possible. These could be categorised in oppositional terms as conjuring up repertoires of resistance (Hollander, 2015) or simply as numerous smaller, non-oppressive data regimes coming into their own., and yet retaining connectivity *if* they so choose. This would, in effect, pave way to securing and protecting the human, as explained further ahead.

Human Security as Data Protection: Advancing Critical Data Studies

The concept of human security (UNDP, 1994; King and Murray, 2001) seeks to focus on the human as the referent object of security, and not the State or other dominant regimes. In other words, it seeks to go beyond articulations that privilege as state-centric view of security like national security, to subvert its power in favour of the human. While the concept of human security is linked to non-traditional forms of security, in the world of data, human security would mean that the essence and proprietary sense of being human is not usurped by data authoritarianism. It means that the human is not reduced to merely being a subject of corporeal regimes. The essence of being a human could be defined, in effect, as more than the individual, the citizen, the customer, and other kinds of subjecthoods. The focus on the everyday activities of the human, permits an understanding of big data replete with its algorithmic computing apparatus, as a daily human endeavor. It imprints the human in big 'data'.

Human security, as the focal point of Critical Data Studies, in studying data protection, allows to foreground emotive rationality as the logic, with its politics being rooted in the emancipatory project. The human security approach complements the idea of multiple data regimes, since it helps steer clear of bindings to singular regimes of power. It allows for coalition-building, and multi-party cooperation (Johns, 2014). It allows for acquaintance with epistemologies of care and helps understand normative conceptual frameworks in a more nuanced manner, thereby allowing us to go beyond deterministic accounts of data institutionalism.

Studies on data protection then, should be rooted in interrogating ownership patterns, access of varied kinds, the right to privacy of the

individual and the ability to "fall off the grid", as a means to challenge oppressive and/or colonial data collection mechanisms. Critical Data Studies should draw on these claims, and should stay firmly rooted in human security, to understand sustainable means of leading data lives today.

References

Allen, Christopher. (2016) http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Couldry, Nick, Yu, Jun. (2018). 'Deconstructing datafication's brave new world'. *New Media and Society*. 20(12), 4473–4491.

Couldry, Nick, Mejias, Ulises A. (2019) 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject'. *Television & New Media,* 20(4), 336-349.

Dalton C and J Thatcher (2014) Inflated Granularity: The Promise of Big Data and the Need for a Critical Data Studies. Presentation at the Annual Meeting of the Association of American Geographers, Tampa, Fl, April 9, 2014.http://meridian.aag.org/callforpapers/program/AbstractDetail.cfm?AbstractID=56048

Dalton, Craig, Taylor, Linnet, Thatcher, Jim. (2016). Critical Data Studies: A dialog on data and space. *Big Data and Society*

Dencik, Lina, Hintz, Arne, Cable, Jonathan. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data and Society*

Greenleaf, Graham. (2017). Privacy in South Asian (SAARC) States: Reasons for Optimism.149 Privacy Laws & Business International Report 18-20; UNSW Law Research Paper No. 20. Available at SSRN: https://ssrn.com/abstract=3113158

Greenleaf, Graham. (July, 2013). Nepal's Unknown Data Privacy Law: No Shangri-La, but a First for South Asia. International Data Privacy Law, Vol 3, Issue 4, 2013 ; UNSW Law Research Paper No. 2013-61. Available at SSRN: https://ssrn.com/abstract=2326799

Hollander, Matthew. (2015). The repertoire of resistance: Non−compliance with directives in Milgram's 'obedience' experiments. British Journal of Social Psychology, 54 (3)

Johns, L. (2014). A Critical Evaluation of the Concept of Human Security. E-IR

King, Gary, Murray, Christopher. (2001). Rethinking Human Security. Political Science Quarterly, 116 (4)

Newman, Nathan. (2015). Data Justice: Taking on Big Data as an Economic Justice Issue

Nissenbaum, Helen. (2017). Deregulating Collection: Must Privacy Give Way to Use Regulation? Available at SSRN: https://ssrn.com/abstract=3092282 or http://dx.doi.org/10.2139/ssrn.3092282

Taylor L (2016) No place to hide? The ethics and analytics of tracking mobility using mobile phone data. Environment and Planning D: Society and Space 34 (2): 319-336

Taylot, Linnet (2017) What is data justice? The case for connecting digital rights and freedoms globally. Big Data and Society

Tobin, Andrew, Reed, Drummond. (2017) The Inevitable Rise of Self-Sovereign Identity. Sovrin Foundation. https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

UNDP. (1994). Human Development Report. Oxford University press: Oxford