Editorial for September 2021 issue

S. V. Raghavan¹

Published online: 11 December 2021
© CSI Publications 2021

Chief Editor: S V Raghavan

The September 2021 issue in your hands carries a series of interesting articles in the broad area of Data Governance, more importantly about Data Privacy and Protection. As Information Technology evolved, one of the domains that benefitted most was the Financial Transaction. In finance related domain, many activities such as banking, insurance, securities, micro-financing, and electronic commerce befitted immensely benefitted and scaled in volume and geographical coverage. Alongside many issues related to jurisdiction, responsibility resting, dispute resolution, scenario re-creations, etc. gained importance. The recognition that policies relating to financial activities across domains of activity and sovereign boundaries started becoming a dominant concern of the finance managers of all hues and shades. The key element however remained as to “How the Data is Handled”.

✉ S. V. Raghavan
sv.raghavan@gov.in

¹ Chennai, India

When close to 1.5 Billion people go online, it is nightmare for any actor, including the regulator. Especially when intense usage comes from unexpected quarters, the ICT designer and the Policy Gurus face the problem of complexity of the system coupled with the simplicity expected by the user, which one can call Designers’ Dilemma. Well, what we have is just the beginning and perhaps the tip of the iceberg. In my usual style, it is my pleasure to introduce briefly the seven articles of this issue.

Smriti Parsheera and Rishabh Bailey in their work on ‘*Data Localisation in India: Paradigms and Processes*’ focuses on data localization in India, where the emphasis appears to be mandatory local storage or processing of data within the country. The authors analyse the policy motivations and challenges of data localization, mapping their arguments into three broad categories, viz., civil liberties, government, and economic. Besides, they examine the robustness of the policy processes through which such norms are being introduced in India—the Personal Data Protection Bill, the Reserve Bank of India’s payments directive, and the localization conditions in telecommunication licenses. The authors’ observations in terms of robustness, transparency, and deliberative policy make the article an interesting read.

Vikram Sinha and Sharmadha Srinivasan in their paper on ‘*An integrated approach to competition regulation and data protection in India*’ analyse the situation wherein market power is concentrated in the hands of a few technology firms raising concerns amongst regulators and policy makers around the world. The authors ask a fine question, “whither competition or data protection?”.

Amol Kulkarni and Siddharth Narayan in their article on ‘*Understanding Intermediary Guidelines from the Lens of Consumer Welfare & Encryption*’ bring forth a consumer perspective on the recently notified Information

Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules), in India with focus on Significant Social Media Intermediaries (SSMI).

Amrita Nanda and Astha Kapoor while discussing on ‘*Non-Personal Data sharing—Potential, Pathways, and problems*’ expound the view that collaboration across stakeholders, focus on building technical and infrastructural capacity, incentivising data sharing, and use of pilots as a means to build iterative and durable policy are the way to go. Authors suggest that, it is important for India to invest in fundamental building blocks, underlying jurisprudence, and consultative policymaking, in order to mould a robust data sharing ecosystem.

Dr Rekha Jain and Rajat Mukerji have written ‘*A Critique of the Non Personal Data Governance Framework*’ wherein they observe that in the last decade data has become an important resource which drives innovation in big data and machine learning. But, Privacy concerns, however, impede the use of personal data in many contexts. The emerging idea of Non-Personal Data (NPD)—which comprises either data that does not contain any personal data in the first place, or data from which all personal data has been removed through digital techniques—can be used for driving innovation. The authors critique the report of the Committee of Experts on ‘non-personal data governance framework’ released by the Government of India in December 2020, from different standpoints.

Sachin Lodha and Kumar Vidhani in their work, ‘Challenges in enabling effective Privacy Self-Management’ discuss multiple challenges from data subject’s perspective. The Authors particularly deliberate on the lack of standardization of privacy policy, consent fatigue, Inappropriate consent and granularity of data sharing challenges. Lastly, the Authors briefly outline four core principles that could serve enterprise to create an effective, rewarding and futuristic privacy program.

Prasanth Sugathan and Apurva Singh in their paper, ‘Tracing Encrypted Message: An Analysis of the Law’ deal with Rule 4(2) of the Information Technology (Intermediary Guideline) Rules, 2021 introduced by Government of India ostensibly to regulate misinformation. The paper discusses the legal challenges pertaining with the provision, the right to encrypt as a subset of fundamental right to privacy, and the associated challenges posed by the traceability provision in its effective exercise. The authors conclude by recommending parliamentary oversight over enactment of such provisions, and alternative mechanisms to be adopted by the law enforcement agencies for investigative purposes instead of attempting to invade privacy of

users of encrypted services through measures like the traceability provision.

I would summarise the current issue as a harbinger of changes that are about to sweep the cyber landscape of India.

I am happy to include the observations of the Subject Experts of the September 2021 issue.

Professor S V Raghavan
Chief Editor

1 Subject expert’s editorial

Data Governance: The Emerging Situation in India

The last decade has seen massive growth in the way data is created, distributed, consumed and monetized, with several cross-cutting aspects including protection of personal data, privacy, cross-border data flows, and unlocking data for applications such as AI/ML emerging as topics of concern. Governments around the world have responded with a slew of Data Governance legislation in order to ensure equitable use of data and protect the privacy of citizens, and some of the legislation, such as GDPR, has had trans-jurisdictional effects.

In India too, data has moved from the periphery of the technology discourse to its centre. Several new legislations in the country, in various stages of adoption, have provisions pertaining to data and the current picture is far from clear. While these laws are being developed in an effort to balance the interests of the different stakeholders—ranging from national interests to that of citizens and also the Industry—there are several aspects that are matters of concern for some of the stakeholders.

CSIT’s current Issue on Privacy and Data Protection strives to gather perspectives from eminent practitioners so as to provide the reader with a cross-section of thinking on the current state of data governance in India. The papers presented in this Issue cover the broad gamut of issues related to the theme of Privacy and Data Protection in the Indian context, including the Personal Data Protection Bill which is being drafted, Data Localization, the newly-released IT Rules related to the Intermediary Guidelines, Governance of Non-Personal Data, Privacy at the Enterprise level and issues related to the Encryption debate.

We hope that the issue will help to stimulate the new but fast-developing field of Data Governance in India.

Amrita Choudhury and Satish Babu
Subject Experts