

REGULATION OF NON-PERSONAL DATA IN INDIA: PRIVACY IMPLICATIONS AND GOVERNANCE CHALLENGES

AUTHOR – SNEHA TRIPATHI* & PURNIMA TYAGI**

* STUDENT AT LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN, INDIA

** ASSISTANT PROFESSOR AT LAW COLLEGE DEHRADUN, UTTARANCHAL UNIVERSITY, DEHRADUN, INDIA

BEST CITATION – SNEHA TRIPATHI & PURNIMA TYAGI, REGULATION OF NON-PERSONAL DATA IN INDIA: PRIVACY IMPLICATIONS AND GOVERNANCE CHALLENGES, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (5) OF 2026, PG. 49-53, APIS – 3920 – 0001 & ISSN – 2583-2344.

Abstract

Non-personal data (NPD) regulation has turned out to be a burning topic in the developing digital India. Although a conventional system of data protection has an emphasis on personal information, the growing economic importance of anonymized and aggregated data requires a different form of control. This paper discusses the conceptual underpinnings of non-personal data, classification, and why there is the necessity of governance processes in India. It also discusses the privacy concerns of the possible re-identification of anonymized information and the danger of abuse. The paper is a critical analysis of the recommendations of the Non-Personal Data Governance Committee and how they overlap with current legal frameworks, such as the Digital Personal Data Protection regime. Also, it illustrates issues of data sharing, ownership, economic exploitation and institutional controls. A summary of the paper also reiterates that a solution to this is the development of a balanced regulatory structure that ensures enhancement of innovation whilst ensuring privacy and the interest of the people.

Introduction

There is a tremendous growth of data made by the rapid development of the digital economy, which is turning into a significant economic resource. Whereas the focus on regulatory attention has always been on personal data, non-personal data which refers to those types of data that cannot be used to identify an individual has been increasing in importance because of the potential this data has on being innovative, governing, and economically growing. The discussion of non-personal data regulation in India became the focus of attention after the establishment of the Committee of Experts on Non-Personal Data Governance Framework in 2020.

There are many different types of non-personal data, such as anonymized personal data,

aggregate data, and community-based data based on sharing resources. Such information is important in industries such as health care, city development, artificial intelligence and online retail. Nonetheless, regulation poses challenging matters with it especially in issues related to data ownership, access and fair distribution of benefits.

One of the major issues is that the personal and non-personal data have a vague definition. The development of data analytics and artificial intelligence has already shown that in some cases, anonymized datasets may be re-identified, and this aspect poses a major issue of privacy violation. This makes regulation a bit more difficult because the schemes created to protect personal data might fail to consider the specifics of non-personal data.

The policy of regulating non-personal data in India attempts to minimize the competing interests that drive data-oriented innovation, provide equal competition in the market, and protect privacy. The proposed governance structure lays an emphasis on sharing of information particularly to the community and societal interests whereas it introduces systems like data trustees and data custodians.

The paper will critically look at the Indian regulatory environment of non-personal information with particular interest to privacy concerns and regulation issues. It seeks to determine how the existing and the suggested structures are effective in dealing with the intricacies of data control in a fast-changing online world.

Thematic Discussion

Non-personal data is an idea that has developed, responding to the increased awareness that data, outside the personal aspect, possesses an economic and a societal value that is vast. The necessity to enforce non-personal data in India has been driven by the fact that it is promising in terms of innovation, better governance, and enhanced economic growth. Nevertheless, this has resulted in considerable grey areas especially in the domain of scope, ownership and use of such data due to the lack of a proper legal framework.

To begin with, we should get to know how non-personal data are classified. The Committee of Experts divided non-personal data into three general types, namely, public non-personal data, private non-personal data, and community non-personal data. Government agencies generate public non-personal data, which is usually regarded as a public resource. The personal information which is not private is gathered by non-governmental organizations and usually utilized in business. Non-personal data on communities perhaps the most controversial group of data is that which is associated with a group of individuals or

community, e.g. data about traffic patterns or farming.

On its part, the classification leads to questions of ownership and control. The non-personal data does not have a definite ownership structure as compared to personal data which is, by definition, inseparable with an individual. An example is the community data, a question arises as to whether the data is owned by the people who produce the information, the organization that gathers the data or the community as one. Such ambiguity complicates the process of regulations and leads to the need to establish new ideas, including those of data trustees, who should serve the interests of the community.

Data sharing is also another important issue in non-personal data regulation. The new framework focuses on the compulsory disclosure of data under some conditions especially when it is in the interest of the populace or when it fosters competitiveness. Although this strategy is expected to eliminate data monopoly and fair access, it also brings up the issue of safeguarding proprietary rights and trade secrets. To the companies that invest much in the data collection and processing, they may be unwilling to open out their datasets unless they are fairly protected.

It is impossible to neglect the economic aspect of non-personal data. The processing of data is increasingly being called the new oil and data monetization has come to be a major driver behind the digital economy. The large technology companies in India have huge data under their belt that are not personal, and thus, offer a competitive edge. This control of such data is aimed at reducing the playing field of such data by allowing smaller players and startups to obtain valuable datasets. Nevertheless, it is still difficult to balance innovation protection and promotion of competition.

The consideration of privacy is a major issue as a regulation of non-personal data. Despite the fact that non-personal data is, by definition, one

that does not contain any personal identifiers, the chances of re-identification still exist. Recent developments in machine learning and data analytics have shown that anonymized data sets can be compared to other data resources in order to identify a person. This is disastrous to the supposition that non-personal data is naturally secure, regarding the privacy aspect.

Even the very notion of anonymization is a problematic concept. No uniform standard is deemed to be effective anonymization. Masking, aggregation, and different privacy techniques provide different levels of protection, yet none of them can ensure 100 per cent anonymity. Consequently, the regulation system should touch upon the fact that in certain circumstances non-personal data may turn into personal data.

Non-personal data regulation and personal data protection are the two key aspects in India. Digital Personal Data Protection framework is concerned with the protection of the personal data, whereas it is not a comprehensive approach towards the issues pertaining to the non-personal data. This has a loophole in regulation particularly in the instances where personal data is transformed into non-personal data by undergoing anonymization. To have both regimes in harmony, there is need to have a cohesive approach.

Another issue in governance is seen in institutional mechanisms suggested to control the non-personal data. The entry of other entities like data trustees and data custodians increases the regulatory game. Although the roles are designed to guarantee accountability and fair use of data, in the real-life situation, they create doubts on jurisdiction, powers, and rules.

The other problem is also in the implementation of data sharing requirements. Obligatory data exchange needs a strong institutional structure that has the ability to track the compliance and address controversies. Without such definitions, it might result in arbitrary decision-making and overreaching of the regulations. Moreover,

international character of data flows makes the process of enforcement more difficult as the data created in India can be stored or processed elsewhere.

The problem of cross-border data flows specifically concerns the case of non-personal information. Whereas personal data is usually localized, non-personal data might not be so. This opens data exchange possibilities all over the world and causes some concerns regarding the sovereignty of data and national security. The process of non-personal data regulation in India should thus take into account the implications of the cross-border data transfers.

The other important aspect of the governance of non-personal data is the ethical considerations. Data being utilized to address artificial intelligence and predictive analytics among other purposes is a question of bias, fairness, and accountability. Any non-personal data, especially those based on community data, can be an indicator of social inequalities that exist. Otherwise, such data can be used to perpetuate or increase these inequalities.

In addition, the regulatory framework should also concern the issue of transparency. The practices regarding data collection and processing are usually obscure and the stakeholders cannot comprehend how their non-personal data is being utilized. To gain trust and have responsible usage of data, it is also important to increase its transparency.

Another issue is the role of the state in controlling non-personal data. Although the intervention of the government is crucial in creating a level playing field and making sure that all people receive their fair share, over-regulation may induce deterioration of innovation and discourage investments. The difficulty here is to make an effective and flexible framework so that it is adaptable to the changes in technology.

Besides domestic implications, India should also be able to synchronize its non-personal data control with the international ones. A lack of a

universal agreement on the governance of non-personal data does have its challenges as well as opportunities. India can become a pioneer in this area by creating a strong and prospective framework.

The liability factor, in relation to non-personal data is also a key issue. Liberty of data misuse or re-identification is not always easy to discern. Responsibility is difficult to give as there are many stakeholders that include data collectors, processors and data users. An open liability system is needed to provide responsibility and discourage wrongdoing.

Lastly, the regulation of non-personal data requires implementation to be successful. It involves not only a good legal framework but also the establishment of technical infrastructure and institutional capacity. Activities that should be supported by capacity-building efforts such as training and awareness creation should be undertaken to maintain regulatory compliance by the stakeholders.

To sum up, the Indian non-personal data regulation is a significant and complicated combination of legal, economic, and ethical regulations. Although the suggested framework suggests an all-encompassing approach, its effectiveness will be based on the possibility of managing the challenges mentioned above. A regulatory balance and dynamism are needed to utilize the potential of non-personal data without interfering with privacy and the general interest of the populace.

Conclusion

The Indian non-personal data regulation is a major step towards the quagmires of the digital economy. With the data becoming more of an important economic asset, the necessity of an elaborate governance structure becomes more and more obvious. This paper has shown that non-personal data is a complex phenomenon, which involves the problems of categorization, possession, accessibility, and economical usage.

Among the most important things that can be found is that the difference between personal and non-personal data is not a definite one. The threat of re-identification arguments contradicts the expectation that non-personal data does not have privacy issues in its nature. This highlights the need to incorporate privacy protection in non-personal data regulation despite the fact that it is anonymized.

The governance issues presented in this paper such as the requirement to share data, institutionalism, and enforcement problems demonstrate that controlling an ever-changing field is not an easy task. Though the suggested framework does present some novel ideas like the idea of data trustees and a compulsory nature of information sharing, it must be applied with precaution to prevent its unforeseen application.

Moreover, the economic essence of the non-personal data regulation raises the necessity to overcome the competing interests. Enhancement of innovation and competition should go hand in hand with the safeguarding of proprietary interests as well as equitable allocation of gains. This balance is essential to the creation of a sustainable and inclusive digital ecosystem.

Finally, the Indian strategy on the non-personal data control should be active and progressive. With the consideration of privacy concerns and the reinforcement of the governing systems as well as being in line with international norms, India will be in a position to have a stronger framework, which will ensure the economic growth and well-being of the society.

References

1. Committee of Experts on Non-Personal Data Governance Framework, *Report* (2020).
2. Ministry of Electronics and Information Technology, *Draft Non-Personal Data Governance Framework* (2020).
3. Justice B.N. Srikrishna Committee, *A Free and Fair Digital Economy* (2018).

4. Digital Personal Data Protection Act, 2023 (India).
5. Information Technology Act, 2000 (India).
6. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L.J. 677 (2015).
7. Paul Ohm, Broken Promises of Privacy, 57 UCLA L. Rev. 1701 (2010).
8. Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Datasets, IEEE (2008).
9. OECD, *Enhancing Access to and Sharing of Data* (2019).
10. World Bank, *World Development Report: Data for Better Lives* (2021).
11. Nandan Nilekani, Data to the People, *Foreign Affairs* (2018).
12. Rohit Chopra & Lina Khan, The Case for “Unfair Methods of Competition”, Yale L.J. (2020).
13. European Commission, *Data Governance Act* (2022).
14. GDPR, Regulation (EU) 2016/679.
15. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
16. Shoshana Zuboff, *The Age of Surveillance Capitalism* (2019).
17. Julie E. Cohen, *Between Truth and Power* (2019).
18. Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).
19. Solove, Daniel J., *Understanding Privacy*, Harvard University Press (2008).
20. Priscilla Regan, *Legislating Privacy* (1995).
21. MeitY, India Data Accessibility and Use Policy (2022).
22. UNCTAD, *Digital Economy Report* (2021).
23. McKinsey Global Institute, *The Age of Analytics* (2016).
24. Reserve Bank of India, *Report on Digital Payments* (2019).
25. NITI Aayog, *National Strategy for Artificial Intelligence* (2018).