International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 29-09-2024, Accepted: 30-10-2024, Published: 14-11-2024
Volume 10, Issue 6, 2024, Page No. 29-31

The necessity of data protection laws in India and the role of blockchain technology in enhancing data security and legal compliance

Sudipta Ranjan Sahoo
Department of Law, MATS School of Law, MATS University, Raipur, Chattisgarh, India

Abstract
Information is now considered as a currency in the information technology era, which makes personal and sensitive information security a priority. Being one of the biggest economies in the digital world, India has numerous issues regarding the protection of citizens' information in the context of the growing technological progress. The Personal Data Protection Bill (PDPB) which is still a bill, is intended to protect personal data in terms of collection, processing and storage, in a very significant step towards data protection. However, today's cyber threats are more complex and developing new technologies like blockchain are important in strengthening the data protection. This paper also focuses on the need for data protection laws in India, impact of blockchain on compliance and data protection and how blockchain can be used to identify people who are infringing data protection laws.

Keywords: Data protection, blockchain technology, legal compliance

Introduction

The evolving digital economy of India means there is an exponential rise in the amount of personal and sensitive information being gathered, analysed, and archived. Since purchasing and banking to healthcare, communication, and government processes, data is a foundation of contemporary business, interaction, and administration. This exponential increase has also led to exponential increase in the risks associated with data misuse, breach and unauthorized access.

However, the Indian government came up with the Personal Data Protection Bill (PDPB) to provide for the legal regime for the collection and processing of personal data. However, issues to do with data protection are still very relevant and prominent, particularly in a world where cybercrimes and privacy invasions are the order of the day.

Therefore, blockchain technology, which is regarded as decentralized and secure technology, offers a solution to these challenges. Blockchain can transform data protection and help the legal profession ensure compliance with data regulations by providing higher levels of transparency, security and traceability.

This paper aims at finding out why there should be laws on data protection in India, the use of blockchain in enhancing data protection, and how it can be used to point out anyone who will have breached the laws on data protection.

The Necessity of Data Protection Laws in India

The rapid use of data has raised the demand for a proper legal framework for data protection. If not properly managed or utilized, personal data is capable of causing serious violation of the privacy of the individuals, identity theft and fraud. Risks associated with cyber-attacks are increasing globally and India has experienced many serious data leakage incidents. Therefore, the Personal Data Protection Bill (PDPB) was introduced in 2019 for to safeguard the citizen's data and to regulate the processing of such data.

1. Key Provisions of the PDPB

The PDPB, based on the General Data Protection Regulation (GDPR) of the European Union, aims to:

- **Regulate data collection and processing**: The bill describes how data should be collected, processed and stored and also explains how individuals' rights over such data should be protected.
- **Ensure transparency**: These aspects mean that organizations have to make people aware of the kind of data being collected, the reason for the collection and the time for which it is being stored.
- **Strengthen consent requirements**: Special care should be taken to ensure that people give their permission before their Personal Data is processed.
- **Create a Data Protection Authority (DPA)**: This body will also be responsible for the exact enforcement of the law, the conduct of investigations and the taking of enforcement action against those organizations that fail to conform to the provisions of the law.
- **Establish data subject rights**: Data subjects will have the right to receive their data and correct it, erase it and none the less, they will also have the right to object to processing the data.

2. Challenges in Data Protection Implementation

Despite these positive steps, India still faces challenges:

- **Vast Digital Infrastructure**: India alone has over a billion people and already over 50% of the population is digitally connected and therefore, the data regulation cannot be a template for the rest of the world.
- **Lack of Data Literacy**: The problem of enforcement of laws is compounded by the fact that a large part of the population in India, including individuals and organizations, may remain unaware of data protection issues.
- **Enforcement Gaps**: Even though the PDPB lays out strong guidelines, its actual implementation depends on the effective enforcement mechanisms, which may require additional resources and technical capacity.

Blockchain Technology and its Role in Data Protection

Blockchain is an innovative technology that has decentralised database and the following characteristics of security and transparency. In principle, blockchain does not need central management, and at the same time, it can provide data distribution among the parties, as well as protection.

1. Key Features of Blockchain that Enhance Data Protection

- **Immutability**: As stated above, once data is recorded in a blockchain, it cannot be altered or deleted without creating proof of the alteration. This characteristic is for the protection of data and it is very hard to forge data keeping it of high standard of security against frauds.
- **Decentralization**: Because blockchain is distributed in nature, there is no one body controlling the system and therefore the threats of a centralized data compromise or a bad actor are minimized.
- **Transparency**: To emphasize, all operations conducted on a blockchain are transparent to all connected individuals in the network. Such transparency can prevent abuse of such data, and is likely to enhance its proper and ethical use.
- **Cryptography**: Blockchain employs complex algorithms to protect data, and the information can only be accessed or changed by permissioned members.

2. Blockchain's Role in Data Protection Compliance

- **Audit Trails**: This architecture of blockchain guarantees the auditability of all data transactions to ensure that accountability of data flow can be tracked in real time. This feature complies with the PDPB requirement of transparency in data processing.
- **Decentralized Identity Management**: Blockchain can allow people to have control over their data, using blockchain for identity management. This would enable people to control who accesses their data, and this would enhance privacy and adherence to data protection laws.
- **Smart Contracts for Data Processing**: Data protection laws must also be integrated into smart contracts – contracts that have their terms of agreement coded into the agreement to self-execute. For example, smart contract implementation may erase personal data processed by the data controller to meet the PDPB right to be forgotten which requires erasing data when it is no longer needed to meet the purpose of processing.

Blockchain and Legal Compliance: Identifying Violations and Enforcing Accountability

Due to its decentralised nature and ability to track information, blockchain is best suited to identify cases of violation of the laws of data protection.

1. Tracking Non-Compliance

Blockchain can help identify and track individuals or organizations that fail to comply with data protection regulations. For instance:

- **Data Access and Breaches**: This way, blockchain enables auditors to know who accessed or modified personal data, when and for what reason every time an access attempt is made. As we know, any intrusion or alteration of the information can be quickly identified.
- **Non-Consensual Data Sharing**: Blockchain may capture when consent is granted for data sharing thus protecting personal data from being used in a way that was not consented. If data is shared without permission, the blockchain record will be proof and action can be taken immediately.

2. Enforcing Compliance and Transparency in the Legal Profession

Legal professionals can use blockchain to ensure that data protection laws are followed in contract management, client data handling, and evidence preservation. Some potential applications include:

- **Digital Contracts and Smart Contracts**: Legal agreements related to data processing can be automatically enforced using smart contracts, reducing human error and ensuring compliance with data protection provisions.
- **Secure Evidence Handling**: Blockchain can provide a secure and transparent mechanism for storing and handling digital evidence in legal proceedings, ensuring that it has not been tampered with.
- **Regulatory Reporting**: Blockchain technology can simplify regulatory reporting by providing real-time, immutable records of data usage, helping organizations meet compliance requirements in a transparent manner.

3. Preventing Fraud and Malfeasance

Blockchain also can be implemented in data processing systems to prevent fraudulent activities like identity theft, data interference or unauthorized use of people's data. This is because blockchain's auditability can potentially eliminate many of the loopholes that the adversaries can exploit to perpetrate unlawful acts.

Conclusion

In view of the fact that digitization in India is happening at an ever-increasing rate, it is essential to have sound legislation on data protection. The Personal Data Protection Bill (PDPB) once implemented, will thus provide a legal regime for the protection of personal data. However, such laws are only effective if they are able to address issues of change in technology and new challenges facing data protection.

As a technology that is entirely transparent, immutable and decentralized, Blockchain can thus be viewed as an effective solution to improve the protection of data and compliance. Blockchain has the potential to support personal data protection by offering a tamper-proof ledger of data exchanges; allowing for decentralised identity management; and using smart contracts to enforce compliance with data protection laws.

To the legal profession, blockchain promises great potential in enhancing the compliance with the data protection laws through the provision of immutable records of data use. It can assist in finding the violators, the cheating and the scams, as well as automating compliance, which in turn, will lead to a safer and more reliable environment and the Internet space.

As India prepares to enforce the PDPB, it is therefore possible that incorporating blockchain technology in the data protection regime in India could go a long way in strengthening the security of citizens' personal data, and making certain that their rights to protection of their data is not compromised especially in the current evolving digital world.

References

1. Government of India. Personal Data Protection Bill, 2019.
2. European Union. General Data Protection Regulation (GDPR), 2016.
3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
4. Tapscott D, Tapscott A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin, 2017.
5. Binns R. Blockchain and Privacy: The Future of Data Protection. Journal of Law and Technology,2018:27(3):312-326.