INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

BLOCKCHAIN AND DATA PROTECTION IN INDIAN HEALTH INSURANCE: LEGAL ISSUES OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

AUTHORED BY - UTHARA J
LLM (Banking and Insurance Law),
Amity Law School, Amity University, Noida

1. Abstract

This growing digitization of the health insurance industry in India has prompted the consideration of new technologies like blockchain to improve its efficiency, transparency, and fraud prevention. With its decentralized and immutable design, blockchain-based systems have a great potential in terms of streamlining claims processing, enhancing the data interoperability, and minimizing the administrative costs. Nonetheless, such technological solutions are subject to the important legal issues that one can consider through the prism of the Digital Personal Data Protection Act, 2023.

The present paper explores the natural conflict between a key feature of blockchain the lack of immutability and the principles of data security found in the Act, especially the right of data principals to amend and to remove personal data. It claims that the conflict is not incidental but structural and has been predetermined by the fundamental incompatibility of decentralized technological systems and rights-based legal frameworks of dealing with personal data.

With a doctrinal review of the statutory provisions and of regulatory law practices, and relational comparison to international data protection regimes, the paper assesses the compatibility of the use of blockchain to health insurance systems with current legal requirements. The paper also discusses how the regulatory bodies such as the Insurance Regulatory and Development Authority of India have helped to deal with these issues.

The article makes a final suggestion of a hybridized approach concerning the formulation of the model of compliance and proposed to combine technological alterations in design with the reorganization of legal and regulatory statutes, which would allow responsible blockchain integration into the Indian health insurance system and protect the privacy of individual

ISSN: 2582-6433

individuals.

Keywords: Blockchain Technology, Data Protection Law, Health Insurance Regulation, Digital Personal Data Protection Act, 2023, Right to Erasure

2. Introduction

2.1 Background and Context

The increasing digitization of financial and medical services has been a major to the changes in the operational landscape of India in the insurance industry. The growth of health insurance, especially, has been significant as more people are becoming aware of the costs of healthcare as well as the efforts of the government in raising coverage. This has been coupled with the incorporation of modern technology to increase efficiency, minimize fraud, and optimality in administration.

One of such technologies is blockchain, which has become one of the roots of promising innovations that can resolve the issues of the insurance industry that have long been there. In India, health insurance schemes have traditionally been marred by challenges like asymmetry of information, and claim settlement, fraudulent allowable claims, and failure to interoperate between the stakeholders like insurers, hospitals and third party administrators. The issue of decentralized and resistant architecture of blockchain technology is a promising solution that has the opportunity to design a transparent and reliable ecosystem in which data can be safely exchanged and authenticated on the fly.

The adoption of such technologies however is not in a regulatory vacuum. The growing dependence on the digital procedures in formalizing sensitive personal and health-oriented information has led to the need to enact exhaustive data protection legislation. In India, it has been responded to by introducing such a need into the Digital Personal Data Protection Act, 2023, which creates a rights-based system of disposing of personal data, its processing, and storage.

2.2 Introduction of blockchain in health insurance

Having initially been designed as a backbone of cryptocurrencies, blockchain technology has developed into a flexible tool and can be used in various industries, such as finance, supply chain management, and healthcare. Blockchain is becoming considered in the context of health insurance due to its potential to promote transparency, minimize administrative drawbacks, and facilitate the safe distribution of data.

ISSN: 2582-6433

Among the main applications are automated claims processing with the help of smart contracts, detecting fraud with the help of immutable records of transactions, and building unified health data repositories, which may be accessed by authorized stakeholders. They are specifically applicable to the Indian context where there has been a long period of inefficiency in healthcare induced by the disjointed healthcare systems, and the lack of standardized means of sharing data.

However, regardless of its benefits, blockchain presents special legal challenges. Its decentralized design obstructs the classical approaches to regulation based on recognizable data controllers or intermediaries. What is even more important is that blockchain records cannot be changed or even deleted once they are entered thus seriously concerning the laws of data protection that prioritizes the rights of individuals over individual data.

2.3 Data Protection Regulation Rise in India

The enactment of Article 21 in the Constitution recognizing privacy as a basic right has played a key role in the development of the law of data protection in India. The introduction of the Digital Personal Data Protection Act, 2023, is a groundbreaking step in such a direction, offering a set of practices covering the protection of personal data.

The Act also sets certain principles that include lawful processing, limit purpose, minimal data, and duty of data fiduciary. It also provides individuals (data principals) with certain rights, such as, the right to access information, correct inaccuracies and demand the deletion of personal data. These entitlement are fundamental to guarantee personal freedom and dominion over personal data.

In health insurance business, where personal and medical information is highly sensitive, and where such information is processed regularly, adherence to these principles is paramount. Insurers, hospitals, and intermediaries must make sure they have effective data security and that the personal data is handled in a legally and transparent way.

2.4 Study Scope and Objectives

The present study lies at the intersection of technology and law with a narrower focus on the utilization of blockchain technology in India in the field of health insurance and its suitability with the data protection regulations in the Digital Personal Data Protection Act, 2023.

The main aim of the paper is to discuss the legal tensions in the context of using blockchain systems to process personal health data. It aims to examine how the intrinsic nature of blockchain, especially immutability and decentralization can be made compatible with such

ISSN: 2582-6433

statutory provisions as the right to correction and erasure of personal data.

The research will also determine the regulatory loopholes and the shortcoming in the present day legal system like the contribution of the sectoral regulators (Insurance Regulatory and Development Authority of India) towards discussing the technological innovations. The paper has attempted to introduce a middle-way solution which encourages technological innovation and protects the basic privacy rights by integrating comparative lessons of other jurisdictions.

Lastly, this study also relates to the larger discussion of how legal systems may evolve with new technologies, without altering fundamental ideals of justice, accountability, and personal autonomy.

3. Research Problem

3.1 Nature of the legal issue

The key research question of, this paper is based on a major contradiction between the technological design of blockchain systems and the stipulations of the legal framework related to data protection in the Digital Personal Data Protection Act, 2023. The nature of blockchain is to provide immutability i.e. once the information is stored in the ledger one cannot change it or delete it. This characteristic is vital to the preservation of trust, transparency and integrity in decentralized systems.

Conversely, the DPDP Act is based on a rights-oriented model that puts an emphasis on personal data control by an individual. It allows the data principals the right to remedy falsely presented data and demand the deletion of personal data provided that there are specified conditions. These rights are not its mere procedures but the essence of the informational self-determination and privacy protection.

The struggle is no coincidental, though, but structural. The immutability of blockchain has a direct negative effect on the enforcement of legal rights which need to amend or destroy data. Considering such sensitive personal and medical information is being processed in health insurance, this tension is especially acute. There are no easy ways of correcting inaccurate medical records or outdated health information and once they are stored on a blockchain, there is no easy solution to deleting them.

3.2 Technology–Law Disconnect

Another important aspect of the research problem is the lack of the connection between a technological design and legal expectations. Blockchain systems are designed in a way that frequently places efficiency, security, and decentralization and little to no thought on legal

ISSN: 2582-6433

compliance requirements. On the other hand, data protection regulation is developed in accordance with more traditional data processing paradigms which presuppose the importance of identifiable controllers of data who will be able to alter or destroy data.

This matter poses a regulatory loophole. It could prove challenging to find a single data fiduciary in the case of health insurance systems based on blockchain because compliance with the Digital Personal Data Protection Act, 2023 has to be enforced. Blockchain is a decentralized technology that has its power divided among various nodes, casting doubt on accountability, liability, and enforcement.

Additionally, possible solutions that have been offered like encryption or off-chain storage, although many times deserved as a solution, do not fully address the issue of law. As an example, although the personal data are encrypted, their preservation in the blockchain may still contradict the data erasure principle. On the same note, the storage of data off-chain brings fresh threats in terms of security, integrity, and regulatory risks.

3.3 Relevance of the Problem to the Indian context

This research problem is especially relevant to India as the digital health infrastructure and insurance coverage are growing at a rapid pace. There is a move towards the usage of digital technologies, which are fostered by government initiatives and innovation in the private sector towards the provision of enhanced access to healthcare and insurance services. The use of blockchain in health insurance systems seems increasingly feasible as the trend of its use increases.

Meanwhile, the introduction of the Digital Personal Data Protection Act, 2023 illustrates that India is determined to ensure proper protection and the privileges of data protection and privacy. The intertwining of these two trends, technological innovation and legal regulation, has resulted in a complicated arena, in which conflicts cannot be avoided.

Lack of explicit regulatory directions on how to use blockchain in sensitive sectors like health insurance worsens the issue. Although the Insurance Regulatory and Development Authority of India is very vital in regulating the practice of insurance, little is clear on how emerging technologies are to be regulated under the current legal religions.

This indecision is implicationally more extensive. It can impede innovation because it presents legal risks to the insurers and technology providers as it also leaves people vulnerable to the threat of having their privacy rights violated. Thus, this research problem is vital to not only be addressed in order to achieve legal clarity but also to guarantee the existence of a balanced approach towards the development of technologies and protection of rights in India.

ISSN: 2582-6433

4. Research Questions And Hypothesis

4.1 Research Questions

The research questions presented in this study are a number of closely interrelated questions that attempt to look at the legal and regulatory concerns of the use of blockchain technology in the Indian health insurance market. These interrogatives are structured so as to look both into the inconsistencies of the doctrine and the implications in practice of the Digital Personal Data Protection Act, 2023.

The major research questions are the following:

How does the immutability of blockchain violate the rights to data protection provided by the Digital Personal Data Protection Act, 2023, especially the right to correction and erasure?

Is it possible to design blockchain-based systems of health insurance in a way that will make them highly accountable in terms of meeting the data protection requirements of India statutory laws?

What is the impact of the decentralized quality of blockchain in terms of data fiduciary identification and liability under Indian data protection law?

What should sector-specific regulators, like Insurance Regulatory and Development Authority of India, do with the legal issues emerging due to new technologies?

So, what do comparative jurisdictions teach us, more so those jurisdictions that undoubtedly are taking the GDPR-like routes, which are how to reconcile blockchain with data protection laws?

All these questions are to evaluate the adequacy of the current legal framework to control the application of blockchain in health insurance or whether major reforms are needed.

4.2 Hypothesis

H1: Health insurance systems with blockchain technology, as they exist today, do not comply with essential data protection rights, especially rights to rectify and be forgotten, under the Digital Personal Data Protection Act, 2023.

The premise underlying this hypothesis is that the very nature of blockchain (immutability) contradicts legal demands to alter or eliminate personal data. The assumption of this hypothesis is that this conflict is not a technical but a structural one that cannot be effectively solved by providing some technical modification of the situation or by choosing an interpretation within the existing legal system.

This hypothesis can be tested through a doctrinal study of statutory clauses, an analysis of blockchain architecture and an analysis of whether compliance mechanisms can practically be

ISSN: 2582-6433

rolled out of the blockchain systems without disrupting the functionality of the underlying blockchain.

H2: A hybrid regulatory and technological response that includes privacy-by-design key to addressing the issue of blockchain technology and data protection law in India as well as adaptive regulatory interpretation and sector-specific regulatory guidance can alleviate the conflict between blockchain technology and the law on data protection in India.

The test of this hypothesis will need a critical review of the current technological solutions, regulatory frameworks, as well as comparative legal methods. It equally is the study of the possibility of such hybrid model to strike a good balance between innovation and issues to do with the protection of individual rights.

5. Conceptual and Theoretical Framework

5.1 Blockchain Technology: Characteristics and Legal considerations

The blockchain technology is a type of a distributed ledger that allows recording transactions in a network of computers in such a way that it becomes transparent, secure, and resistant to manipulations. In contrast to the conventional centralized databases, blockchain has a decentralized structure in which no one person has total control of the data. All transactions are authenticated by consensus ensures and each is stored in cryptographically validated blocks with links to the other creating an immutable chain.

The main characteristics of the blockchain, such as decentralization, immutability, transparency and security, carry strong legal repercussions. The notion of decentralization presents issues with the traditional regulatory paradigms based on the presence of clearly recognizable intermediaries or data controllers. Control in blockchain networks is frequently spread between various parties and it becomes hard to allocate a responsibility or liability.

The most typical feature of blockchain is immutability that guarantees that once data are registered by the system, it cannot be changed or removed. Although this aspect helps to increase trust and avoid fraud, it presents severe issues in legal terms when the data needs to be changed or erased. The failure to correct or delete the data can result in the contravention of the laws and regulatory requirements in the health insurance industry because the data processed in this field is very sensitive, and includes both personal and medical information.

Another building block is transparency where participants in the network can access and verify transactions. But this poses the questions of privacy and confidentiality especially with regards to sensitive health information. Although the information is pseudonymized or encrypted the possibility of re-identification cannot be completely reduced.

ISSN: 2582-6433

Therefore, although blockchain has substantial technological benefits, its characteristics place intrinsic strains on the current legal framework, especially laws that regulate data protection and privacy.

5.2 Data Protection Principle of the Digital Personal Data Protection Act, 2023

Digital Personal Data Protection Act 2023 has created a universal guideline documenting the safeguards of personal information in India. It is based on the rights-focused approach which focuses on the autonomy of individuals, responsibility of data handlers and legal processing of personal data.

The main principles of the Act are:

Legal Processing: Individual data need to be handled legally and with authorization or other legal reasons.

Purpose Limitation: Collection of data must be done based on defined, clear and lawful purposes with which data should not be used.

Minimization of Data: A collection and processing of data must be done based on only that data which is essential to the research purpose.

Models: Data fiduciaries must make sure that personal data is both accurate and updated.

Storage Limit: Personal information must not be stored longer than is necessary.

Accountability: Data fiduciaries should have proper protective measures in place and their adherence to the law should be shown.

Along with these principles, the Act provides data principals with a number of rights, such as the right to access information, correct inaccuracies and request the erasure of personal data. All these rights play a central role in making sure that people have the control over their personal information.

The use of these principles within the framework of blockchain-based systems also brings up complicated legal considerations. An example is that the principle of minimum data could be at odds with the practice of storing detailed transaction information on a blockchain. Equally, the need of precision and the right to correction are hard to implement in systems without the possibility to modify data.

5.3 Informational Privacy and Constitutional Aspects (Article 21)

The development of the idea of data protection in India is most strongly connected to the constitutional aspects of privacy as the right of the first order expressed in Article 21. Informational privacy is an aspect of this right that is defined as the capacity of a person to

ISSN: 2582-6433

regulate the gathering, use and communication of personal information.

This acknowledgement of informational privacy duty obligates the State to make sure that the data protection laws are developed and enforced in a way that protects the personal autonomy and dignity. It further provides that privacy should be interfered with so as to justify it under the grounds of legality, necessity, and proportionality.

Informational privacy is especially very critical in the context of the health insurance. Health information is sensitive in nature and may expose confidential information about a physical and mental state of a person. Illegal access, misuse or possession of such data may lead to severe impacts such as discrimination, stigmatization and even economic damage.

The systems based on blockchain, by definition, bring into question the conventional informational privacy. The storage of the data in both permanent and distributed form could deny a person control over their personal information. Although data is encrypting, the fact that data linger on the network may override the principle that individuals are entitled to give or withhold consent, and request that their data be erased.

Therefore, the constitutional aspect of privacy contributes one more twist to this legal discourse, making it necessary to strike the right balance between technological innovation and constitutional rights.

5.4 Technology vs. Rights-based Legal Frameworks

On a more theoretical level, the contradiction between blockchain and data protection law can be interpreted through the prism of a more profound opposition of technology-oriented systems to rights-based legal schemes. Efficiency, scalability and security are some of the objectives of most technological systems, but other frameworks like the law are based on normative principles of fair treatment, accountability, and safeguard of personal rights.

Blockchain is a paradigm shift in the management and storage of information, shifting towards decentralized control to the centralized one. Nevertheless, the majority of current jurisdiction, such as the Digital Personal Data Protection Act, 2023, is founded on suppositions of centralized data management and recognizable figures to enforce adherence.

This incongruity brings difficulties to the application of old legal notions to novel technological situations. To illustrate, the concept of a data fiduciary presupposes the presence of the distinct organization that is known and delineates the purpose and the way the data is processed. Such an entity could be missing in decentralized blockchain networks, or its identification can be obscure.

Besides, rights-based frameworks focus on the power of individuals to have control over their

ISSN: 2582-6433

data, such as even the right to alter or destroy it. Blockchain, in turn, places a higher emphasis on permanence and integrity of data, and must compromise flexibility.

This conflict brings forth critical issues regarding how adaptable legal regimes will be. Should the laws be redefined so that they fit in the new technology or can the technologies be redefined to fulfil the current legal standards? A compromise between the two probable is the solution which will include some of each without jeopardizing the primary rights through innovation.

6. Health Insurance Mobile Health and Blockchain Use Cases and Legal Relevance

6.1 Processing and Automation of Claims

Automation in claims processing is one of the health insurance applications where the blockchain technology proves to be very important. Historically, the process of claims settlement in India includes several intermediaries, such as; insurers, hospitals and third-party administrators (TPAs) which tend to lead to delays, inefficiencies and disputes. The system is further complicated by manual verification procedures and absence of standardised documentation coupled with information asymmetry.

To automate this process, blockchain technology can make it a shared, immutable ledger, which all authorized stakeholders can access. By using smart contracts, which are software programs that run automatically in the blockchain, claims can be automated when a set of defined conditions are met. To give an example, when a hospital has uploaded valid treatment details, the system would issue automatic claim payments without the system requiring any manual adjustments.

Legally, this casts significant issues about accountability and compliance. Automated decision-making can reduce the possibility of policyholders being able to appeal the decision on a claim, especially when the rationale contained in the smart contract is non-transparent. Also, misleading or inaccurate data entry or algorithm creation can lead to either approvals or rejections of claims, and there is no easy way to resolve them, given that blockchain entries can never be overturned.

They should be considered based on the duties outlined in the Digital Personal Data Protection Act, 2023, especially the need to assure that the personal data is accurate and provided with avenues of rectification.

ISSN: 2582-6433

6.2 Fraud detection and Risk Assessment

Addressing gross malpractices and improper claims has always been a significant issue in the health insurance industry and it has cost policyholders money and higher premiums. An effective solution to this issue relies on blockchain technology which keeps an open and unchangeable history of all transactions and it would be much harder to tamper or corrupt information.

Combining blockchain with sophisticated analytics and artificial intelligence, insurers will be able to recognize the trends that could be related to fraudulent activities, including the occurrence of multiple claims to the same treatment or discrepancies between medical records. The common ledger allows various actors to detect the validity of claims, thus, minimizing the fraud threats.

Nonetheless, there is also a concern regarding the privacy when such systems are used. Constant observation and analysis of individual health information could result in the intrusion in data processing mechanisms. The combination of bulk amounts of sensitive information raises the threat of unauthorized access and abuse.

Within the framework of the Digital Personal Data Protection Act, 2023, these kinds of processing should be based on the principles of purpose limitation and data minimization. The difficulty is to strike between the significance of developing effective ways of detecting fraud and the necessity of ensuring the privacy of individuals. The over-collection of data or long-term storage of data to aid in detecting fraud could be against the law.

The sharing of health data and its interoperability involve digital information and are referred to as digital health.

One never-ending problem in the Indian healthcare sector is the dis-inter operability amongst various stakeholders. Medical records are also divided between hospital, clinics, and insurance companies; thus inefficiencies and redundancy of services occur in in these areas. The blockchain technology transactions can directly help in streamlined data sharing by establishing a single and safe platform through which trusted parties could get access to authenticated health records.

This can greatly enhance underwriting accuracy, claims processing as well as the customer experience in the context of health insurance. Insurers are able to obtain real time information to evaluate risk better, and policyholders enjoy quicker and more effective services.

But the legal aspect of such shared data is huge. The health information is categorized as containing highly sensitive health data, and its processing should follow the norms of data protection strictly. Decentralization of blockchain makes it difficult to enforce access controls

ISSN: 2582-6433

and consent management mechanisms.

The Digital Personal Data Protection Act, 2023 underlines that it is of vital importance that the data is shared, only with the concerned parties, and under the purpose that it is justified. Moreover, the data published on a blockchain is difficult to regulate in its further utilization, which makes the unethical processing of the data and its possible application possible.

6.3 Insurance Smart Contract

Smart contracts are a disruptive blockchain technology in the insurance industry. They are self-enforceable contracts whereby terms and conditions are coded in software programs, which run automatically upon meeting pre-specified conditions. Smart contracts may be applied in health insurance to make premium payments and policy renewal, as well as claims settlement, automated.

The utilization of smart contracts has a number of benefits such as decreased administrative fees, the removal of meddlers, and greater effectiveness. They are, however, of questionable legality and enforceability under Indian law. The questions that arise are whether the smart contracts are valid contracts according to the current legal framework and specifically in terms of consent, interpretation, and dispute resolving.

Additionally, inflexibility of smart contracts becomes a problem when it is necessary to have flexibility or human decisions. As an illustration, the extraordinary conditions or vagueness of the terms of policy cannot be sufficiently dealt with by the automated systems. Failure to change or revoke the running of smart contracts can be unfair.

Data protection wise, smart contracts are usually based on constant access to personal data to be effective. This casts doubt upon the extent of consent, restriction on purpose, and retention of data. Such systems must have sufficient protection measures to safeguard individual rights in accordance with the Digital Personal Data Protection Act, 2023.

7. Indian Law that regulates Data Protection

7.1 General overview of the Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), is the first Act in India that focuses on the safety of personal data. It sets a legal framework on the collection, processing, storing and transfer of digital personal data, prioritizing on individual rights and the institutions accountability.

The Act is applicable to the modes of processing digital personal data in India and in some instances which I will discuss, to the modes of processing outside India when these are linked

ISSN: 2582-6433

to the services or provision of goods to people in the country. It takes a consent-centric approach whereby handling personal data should be upon the free, knowing, particular and expressed permission of the data principal, except in the event of legitimate use as outlined in the Act.

One of the notable aspects of the DPDP Act is its adaptable and principle-oriented nature, enabling flexibility to changes that come with the evolving technologies. Nonetheless, this also offers interpretative problems, especially when translating the law to decentralized systems like the blockchain. The Act presumes that there exist identifiable entities processing data, which might not go hand in hand with the decentralized blockchain network.

7.2 Rights of Data Principles

DPDP Act gives much importance to the rights of the person also known as data principals thus acknowledging their autonomy and rights to the personal data. These rights are the foundation of the Act and without them accountability and transparency in the data processing will not be available.

Key rights include:

Right to Access Information: Data principals have the right to access information pertaining to how their personal data is processed, the purpose and type of data processed.

Right to Correction and Erasure: individuals with the right to ask that their personal data be corrected or (sometimes) erased when it is not necessary to retain the data (the initial purpose of its collection).

First, Right to Grievance Redressal: Data principals have every right to proper infrastructure on how to solve the complaint in data processing.

Right to Nominate: principle people are able to nominate another individual to nutrient their rights in case of death or incapacity.

One of them, the right to correction and to erasure, is especially applicable to the context of blockchain. These rights entail that the data fiduciaries must alter or destroy personal data when requested but under some specific conditions. Nonetheless, such obligations might be hard, or even impossible, when considering the technical architecture of the blockchain.

Data fiduciaries have the following obligations:

The DPDP Act imposes a set of responsibilities on the entities which define the destination and methods of processing personal data called data fiduciaries. These commitments are created to guarantee accountable data processing as well as to safeguard the rights of the data main participants.

ISSN: 2582-6433

Key obligations include:

Purpose Limitation and Data Minimization: Data fiduciaries are expected to collect only data that is relevant to certain purposes and avoid unnecessary and excessive data gathering.

Accuracy and Completeness: Significant efforts should be made to do all the available to verify that personal data is accurate and up to date.

Storage Limitation: The data is not to be stored longer than the required time to serve the purpose that is determined.

Security Safeguards: Proper technical and organizational safeguards should be put in place to guard against breaches of personal data.

Responsibility: The data fiduciaries would have to show that they have met the stipulations of the Act.

The compliance of these obligations has special criteria in systems based on blockchains. To take an example, data minimization may not be compatible with the necessity to keep records of all transactions. Equally, the necessity to erase information after some time is challenging to align with an unchangeable blockchain storage.

The very notion of data fiduciary is obfuscated in decentralized networks, when various actors can reach a consensus on how to process data without a clear order and without an overall figure of authority.

7.4 Regulatory and Development Authority of India In Health Insurance

Besides the DPDP Act, the health insurance industry in India is under regulations that regulate the industry, under the Insurance Regulatory and Development Authority of India. The IRDAI is mandated with the responsibility of orderly developing the insurance sector, securing the interests of the policyholders and overseeing the practice of insurance.

Although the IRDAI provided the guidelines regarding data management, cybersecurity, and outsourcing, its regulations are yet to comprehensively cover the consequences of such new technologies as blockchain. This gives a loophole in sector-specific regulation, especially in fields dealing with sensitive health information.

The co-existence of the general data protection law and sectoral regulation is critical. The overall legal framework is executed in the DPDP Act, and the IRDAI is likely to come up with specific guidelines that meet the requirements and risk of the insurance sector. Without this guidance, insurers will be at a crossroads in understanding compliance requirements in implementing blockchain-based systems.

Additionally, the IRDAI plays a crucial role in sensitizing that technological innovation should

ISSN: 2582-6433

not affect consumer protection. This encompasses setting transparency and accountability, and also dispute resolution standards in utilizing automated systems and decentralized technologies.

8. Core Legal Conflicts

8.1 Immutable vs. Right to Erasure

The most basic legal conflict between blockchain technology and the law on data protection is related to the relationship between the impossibility of blockchain alteration and the provision of the right to erasure in the Digital Personal Data Protection Act, 2023. The nature of blockchain systems is to provide protection to ensure that once the data has been recorded, data can no longer be removed or altered, without affecting the integrity of the whole ledger. It has this property, which is vital in preserving trust, avoiding fraud, and transparency.

Contrastingly, the DPDP Act enables data principals the right to request erasure of personal data based on some specific conditions especially once the data cease to be required by its intended use, or once consent is revoked. This right plays a pivotal role in the notion of informational self-determination and allows people to have the right to own their personal information.

This conflict is especially problematic in the case of health insurance systems based on blockchain. Once personal health data is stored on a blockchain, it may never leave it, as it can be irrelevant, and it can have been processed illegally. Such data could not be deleted, which directly adversely affected the facade of enforcing statutory rights.

Potential solutions to this problem include some technological solutions, including storing personal data off-chain and storing only hashed references on the blockchain. Yet, these strategies do not handle the problem completely since even the presence of unalterable references can lead to legal ambiguities in terms of further processing of personal data.

8.2 Right to correction vs. distributed ledger integrity

The other important dispute is concerning the right to correction of incorrect or misrepresenting personal information. Digital Personal Data Protection Act, 2023 imposes the data fiduciary responsibility on ensuring that personal data is accurate and up to date, and are giving the ability to correct inaccuracies when requested.

Blockchain systems on the other hand do not allow one to modify the existing records. Although technically it is possible to add in new data that overrides that of the past, the old incorrect data still remains in the ledger of permanence. This questions the legality of such an

ISSN: 2582-6433

approach in meeting the legal requirement of correction.

Considering the situation with health insurance, any erroneous information, which can be any type of incorrect medical history or erroneous records of claims, can cost a person dearly, with a refusal of a health insurance policy or a higher cost. The fact that these inaccuracies can be still found in a fixed form may still influence the process of decision making hence rendering the right to correction ineffective.

This problem emphasizes the inappropriateness of applying the old-fashioned legal concepts to the decentralized systems. Legal concept of corruption presupposes the possibility to update or substitute erroneous data, but blockchain systems are grounded with the integrity of past records.

8.3 Data Minimization vs. Permanent Storage

The data minimization principle means that no more (or less) personal data must be collected and processed than is needed to fulfil a certain purpose. This principle is also unified with the idea of proportionality and intended to restrain unwarranted intrusion into the privacy of individuals.

By its nature, blockchain systems have the propensity to keep detailed information about the transaction so that it can be transparent and traceable. In health insurance practice, this can be a record of the medical treatments, history of claims and stakeholder interaction.

Such data should be stored permanently which brings about the issue of adhering to the principle of data minimization. Although the data might be first targeted towards a reasonable purpose, indefinite storing in a blockchain could be more than what is needed to achieve that purpose. This is especially problematic when the data is no longer needed and the ledger cannot be modified, giving its immutability.

Moreover, privacy is escalated by the potential of data collection and abuse over time due to massive amounts of data being stored.

8.4 Decentralised System Accountability

Another key attribute of data protection law is the term accountability that means that fiduciaries of data must be accountable towards the legal provisions in data protection and remedies in case of any breach. Digital Personal Data Protection Act, 2023 is based on such set of identifiable entities to outline the purpose and method of data processing.

It is poised to be challenged by blockchain systems, notably, public and permissionless networks, which divide control among many participants. This may not have any single party

ISSN: 2582-6433

that can be singled out as the data fiduciary in such systems. Rather, the process of making decisions can be decentralized and involved parties could contribute to the handling of data.

This poses great concerns on the matter of liability and enforcement. In case there is a data breach, or the rights to protect the data are violated, it might be hard to define the person in charge. The lack of a central authority makes it harder to establish a regulative oversight system and redressal in cases of grievance.

The problem of accountability is even more complicated in the health insurance scenario where various parties are to be considered. The operation of blockchain systems can involve insurers, hospitals and technology providers, which makes it difficult to assign a role of complying with data protection laws.

8.5 Cross Border Data Flow Problems

Networks based on the use of blockchains usually have nodes distributed across nation borders and belong to various jurisdictions. This creates issues concerning the intercountry data transfers and the applicability of the national laws that are used to defend data.

The Digital Personal Data Protection Act, 2023 allows for the transfer of personal data outside India subject to certain conditions and restrictions. But on a decentralized blockchain, information can be copied and stored in several jurisdictions, and it is unclear where the information is kept or where it has travelled.

This is highly dangerous in the case of health insurance with sensitive personal data potentially being processed or stored in jurisdictions with varying levels of data protection. It becomes difficult to ensure that Indian law is adhered to in these cases especially when the foreign nodes are involved.

Also, cross-border data flows give rise to jurisdictional, enforcement and conflict of laws issues. The issue of the applicability of the legal framework and the enforcement of rights across jurisdictions is quite a complex issue that should be taken into thorough consideration.

9. Comparative Legal Analysis

9.1 GDPR and Blockchain Tensions

The General Data Protection Regulation (GDPR) of the European Union is commonly considered one of the most complete data protection regimes worldwide and offers an effective model of comparison to understand the challenges brought by blockchain technology. Similar to the Digital Personal Data Protection Act, 2023, GDPR is a rights-oriented approach, which focuses on ensuring that people have control over their personal data, and on imposing

ISSN: 2582-6433

limitations on the users of data in the roles of data controller and data processors.

One of the main conflict areas with the GDPR, like the Indian one, is the incompatibility between blockchain and the right to be forgotten (right to erasure). The GDPR provides that personal information must be deleted in some situations such as; when the same data is not needed to achieve the same purpose that caused its collection or when the data subject objects to it.

The impossibility of using this right in relation to blockchain systems has been pointed out in scholarly discussions and regulatory debates in the EU. As the data written on a blockchain cannot be erased, the right to erasure cannot be adhered to. This has resulted in divergent interpretations with some positing that effective erasure can be attained by using methods like encryption or making the data unusable and others arguing that these methods are not all encompassing of legal stipulations.

Another aspect of the GDPR is accountability, which includes the provision of having data controllers clearly in charge of meeting the requirements. Such entities are difficult to find in decentralized blockchain networks and thus the question of liability and enforcement becomes uncertain.

9.2 Approaches in the European Union

Policymakers and regulators in Europe have taken a conservative and flexible stance towards the intersection of blockchain and data protection. Instead of banning the utilisation of blockchain, the emphasis has been on reinterpreting current legal principles in a way that does not restrain technological advancement, but also critical rights are not infringed in the process. Among them has been the promotion of privacy-by-design aspects, whereby developers have been urged to ensure data protection measures are built into the architecture of blockchain systems. It involves ensuring the reduction of the volume of personal data stored off-chain, its pseudonymization, in addition to efficient access controls.

Another method is the differentiation of the various forms of blockchain networks. Authorized or closed blockchains, in which membership is limited and governance frameworks are better determined, are said to better align with data protection needs than public and permissionless networks. With this, responsible entities are easier to determine and compliance mechanisms can be implemented in such systems.

The notion of functional equivalence considering legal compliance as conflicting with the fulfillment of the goals of data protection laws instead of by strict compliance to certain technical requirements has been discussed also in Europe. By way of example, it might be

ISSN: 2582-6433

functionally equivalent to deletion in some contexts to make data permanently inaccessible by encrypting it.

Nonetheless, though such efforts have been made, considerable uncertainties exist. The question of how blockchain systems are to be regulated according to the GDPR has not been unanimously agreed upon and the absence of a clear way of doing so has remained a problem to the stakeholders.

9.3 Lessons for India

India can learn a great deal about blockchain technology and data protection as it approaches the crossroads of digital personal data protection and blockchain technology in the Digital Personal Data Protection Act, 2023.

First, it emphasizes the need to be flexible and adaptive in the regulation approach. Regulators must not enforce strict limitations that can hinder innovations, but be ready to design frameworks of interpretation that embrace the new technologies without disrupting basic rights.

Second, the privacy-by-design focus also offers a helpful model that could be useful to India. The promotion or compulsory use of data protection safeguards during the design phase could assist in overcoming a clash of the law and meeting the requirements of the law. This would be in line with the greater goals of the DPDP Act, which prioritizes responsibility and good data handling.

Third, specifically, the uniqueness between various forms of blockchain networks is especially pertinent. India can think of encouraging the adoption of approved blockchain infrastructures to sensitive industries like health insurance where regulators and accountability are crucial.

Fourth, the European Union dilemmas are a reminder of how necessary sector-guided directions are. General laws on data protection, though necessary, might fall short of tackling the challenges which are specific to blockchain technology. In the Indian scenario, the insurance regulatory and development authority of India ought to be prolific in crafting guidelines that are specific to the health insurance industry.

Lastly, the comparative discussion shows that the fight of blockchain versus data protection is not an Indian problem, but a worldwide one. This reaffirms why further research, discussions, and cooperation are necessary to come up with effective regulatory solutions.

10. Research and Analysis

10.1 Legal Conflict Analysis Based on Doctrine

Digital Personal Data Protection Act, 2023, when analyzed via a doctrinal approach, can be

ISSN: 2582-6433

noted to be based on the key concepts of control, accountability, and the flexibility in data processing. The principles presuppose that individual data may be changed, limited, or deleted to comply with the exercise of personal rights. Nonetheless, the logic of blockchain technology is the complete opposite one, as it implies permanence, decentralization, and integrity of records.

Such a difference generates an incompatibility of structure. An example is the right to erasure, which cannot be practiced practically in a system, where once the data is stored, they cannot be deleted. The same applies to the right to correction, which could not be effective when erroneous data cannot be fixed but only expanded with some new entries.

On a doctrinal level of knowledge, it becomes clear that the prevailing legal provisions fail to put into consideration the technical limitations of blockchain-based systems. The legislation is based on compliance as possible, and blockchain defies this premise. Consequently, there is a likelihood of making systems relying on blockchain non-compliant or of having to promote the interpretation of legal obligations.

10.2 Gaps and ambiguities in Regulation

The review also points out that there are considerable loopholes in the existing laws. Although the Digital Personal Data Protection Act, 2023 gives them some principles and obligations, it does not specify how to apply these provisions to the emerging technology, i.e., blockchain.

The majority of ambiguities are connected to the officialization of the data fiduciary in decentralized systems. Under conservative data processing models, the third party favoring the processing objective and its modalities is paramount, which is often the data fiduciary. But in blockchain systems, the group may be made up of many participants, that is, it is hard to tell who is in charge of making decisions.

The other gap has to do with lack of clarity in technological compliance standards. Although it requires the adoption of realistic security protection measures, the Act does not dictate the application of such measures in relation to decentralized and immutable systems. This provides uncertainty to those insurers and technology providers who want to adopt blockchain solutions. This also lacks a well-defined role of sectoral regulators in this case like the Insurance Regulatory and Development Authority of India. Even though the IRDAI has the mandate to control the insurance operations, it has not come up with detailed guidelines that deal with use of blockchain in health insurance.

ISSN: 2582-6433

10.3 Compulsions in technologies against legal anticipation

An essential point of analysis is determining whether technological solutions can fill in the gap between blockchain architecture and legal requirements. A number of options have been suggested, such as:

Off-chain storage: Personal information is kept off-chain, and only the references or hashes are stored on-chain.

Encryption and key erasion: Data is encrypted, and key destruction is done by erasing of encryption keys.

Permissioned blockchains: Access is controlled to approved users, and there can be more control and governance.

Though such methods partially resolve the conflict, they are not a complete solution. To give an example, off-chain storage introduces a bit of centralization, which could undermine the advantages of blockchain. Equally, encryption-based solutions might not meet legal requirements of deletion in case the data still exists in any form.

This discussion indicates that technological solutions are inadequate. The opposition between blockchain and the law of data protection is not only technical but also conceptual as it needs to be considered both technically and legally.

11. Recommendations and Suggestions

11.1 Legal and Regulatory Reforms

The discussion in this paper reveals that the current framework as per the Digital Personal Data Protection Act, 2023, though elaborate, does not have all the necessary requirements to tackle the nuances of blockchain technology. Thus, specific legal and regulatory changes are required.

To begin with, the interpretative clarification is required on the use of important rights like correction and erasure with the context of immutable systems. A legislator or regulatory body might want to take into consideration the so-called concept of functional equivalence, which assumes that compliance evaluation is done according to whether the goals of data protection, including the restriction of access or in-usability, are accomplished, despite the fact that it cannot be literally deleted.

Second, there should be definite requirements and definitions of the ways to ascertain responsibility in decentralized systems given by the law. This can include the identification of, or the creation of, more than two parties as joint data fiduciaries or the novel type of responsibility that applies to distributed technologies.

Third, technology-specific regulatory frameworks that will accommodate the distinctive nature

ISSN: 2582-6433

of blockchain are required. These frameworks ought to give specificity regarding what use is allowed, how well it must be adhered to, and what will give rise to uncertainty among stakeholders.

11.2 Sectoral Regulators (IRDAI) Role

In the health insurance sector, the Insurance Regulatory and Development Authority of India would play an important role in narrowing the divide between the advancements in technology and legal requirements.

The IRDAI must come up with sector specific regulations using blockchain to regulate how insurance companies will use the technology especially in claims processing, sharing of information and detection of frauds. Such guidelines ought to cover topics of data governance, accountability, transparency and consumer protection.

Moreover, to allow a controlled experimentation with blockchain technologies, the IRDAI can think about developing a regulatory sandbox system. This would enable insurers and technology providers to explore new solutions but at the same time make sure that their wants are not disallowed by the law and regulations.

Other audit and oversight mechanisms of blockchain-based systems to be stipulated by the regulator should include reviewing data processing practices and algorithmic decision-making that should be done at a regular frequency. This would help in improving the accountability and establish trust between policy holders.

11.3 Privacy-by-Design Approaches

One of the major suggestions that has arisen out of this research is the implementation of privacy-by-design principles in design and execution of blockchain systems. This pattern entails that the protection of data must reflect in the design of technological systems and not as an afterthought.

This may entail:

Reducing the number of personal data logged to the blockchain;

Using pseudonymization and anonymization techniques to protect individual identities;

Putting in place effective access control policies that will make sure only authorized parties can gain access to sensitive information;

Creating mechanisms to enable efficient exercise of the rights of data subjects, despite technical limitations.

Privacy-by-design does not only increase adherence to the Digital Personal Data Protection

ISSN: 2582-6433

Act, 2023 but it also minimizes the possibility of lawsuits and damaged reputation.

11.4 Technological Solutions

Although law change is very important, the use of technology innovation is key towards providing a solution to the identified conflicts. Some technological options may be considered to improve the compatibility between blockchain systems and data protection needs:

Off-chain storage models where personal data is kept off-chain and references of the data are stored on-chain;

Solutions that are based on encryption, with access to data maybe limited through controlled encryption keys;

In more controlled participation and governance: permissioned blockchain networks;

In this way, data pruning and archiving methods that can restrict the availability of outdated or redundant data.

These are not the ideal solutions but can go a long way to mitigate the intensity of conflicts and provide a means to comply with the law.

11.5 Need for Interdisciplinary Regulation

The issues detected in this research shed light on the necessity of an interdisciplinary way of regulation, which requires cooperation between legal professionals, technologists, policymaking authorities, and traders.

Conventional regulatory frameworks, based on an infrastructure of one discipline, are not up to task of handling the complexities of new technologies. Regulating blockchain in health insurance is complex and needs a unified strategy that embraces both the technical and legal considerations.

This can include the creation of multi-stakeholder advisory groups to help advise on the development and implementation of blockchain systems and the development of standard-setting frameworks to encourage best practices throughout the industry.

11.6 Communication

Lastly, is the capacity building and raising awareness of the stakeholders, who are the insurers, regulators and consumers. A lot of the issues that revolve around blockchain and data protection are due to the lack of awareness of the technology and its legal status.

Stakeholders can be aware of their rights and responsibilities and seek to learn the best ways to use technology, which can improve compliance with the Digital Personal Data Protection

ISSN: 2582-6433

Act, 2023.

12. Conclusion

One of the biggest regulatory issues in the changing environment of the Indian digital economy is the intersection between blockchain technology and the law of data protection. This paper has explored the use of blockchain in health insurance industry as well as critically discussed its congruency with the Digital Personal Data Protection Act, 2023.

The paper will show that it is not only a technical conflict between blockchain and data protection law, but it is persistently structural. The characteristic of blockchain of immutability is in direct conflict with important rights to data protection especially to correction and erasure. These liberties, the fundamental ones when it comes to securing the informational privacy and individual autonomy, are not entirely achievable in the traditional blockchain architectures.

The paper has demonstrated though doctrinal and comparative analysis that the current legal frameworks do not have the complete capability to deal with these challenges. Although to a large extent, the Digital Personal Data Protection Act, 2023 offers a solid frame to data protection, its applicability on the case of decentralized systems is questionable. Equally, there is no industry-specific regulation by the regulatory agencies, like the Insurance Regulatory and Development Authority of India that adds to the regulatory uncertainty.

The analysis of the research hypotheses proves that systems of blockchain-based health insurance, as they are, simply do not fit in with some of the essential data protection conditions. Simultaneously, the research recognizes the fact that this incompatibility is not unequivocal. Many of the identified conflicts can be alleviated through a joint effort of technological innovation, regulatory adjustment, and reinterpretation of the law.

The article highlights that a balanced approach to technological progress and data protection should be adopted, and both concepts should not be considered mutually exclusive. Rather, it also proposes a compromise with the implementation of privacy-by-design, sector-based regulation, and multidisciplinary cooperation. This approach would allow responsibly adopting the blockchain technology and protecting core rights.

to summarize, the future of blockchain in Indian health insurance market will rest on the

ISSN: 2582-6433

capacity of legal and regulatory frameworks to keep up with the technological changes. It is crucial to promote not only the innovation but also to safeguard the constitutional principles of privacy, dignity, and autonomy of individuals in the digital era.

13. References / Bibliography

Books

- Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press 2013)
- Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*(Springer 2017)
- Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018)

Journal Articles

- Michèle Finck, 'Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?' (2019) 2 *European Data Protection Law Review*
- Reuben Binns, 'Fairness in Machine Learning: Lessons from Political Philosophy' (2018) *Proceedings of Machine Learning Research*
- Angela Walch, 'The Path of the Blockchain Lexicon (and the Law)' (2017) *Review of Banking & Financial Law*