SVKM'S NMIMS Deemed to be UNIVERSITY

www.lawreview.nmims.edu

NMIMS STUDENT LAW REVIEW

VOLUME VII

MARCH 2025

Cite this Volume as 7 NMIMS L. Rev. (2025)

NMIMS Student Law Review

Volume VII

March 2025

EDITORIAL BOARD

BOARD OF ADVISORS

BOARD OF PEERS

CONTENT EDITORS

Krisha Suri

IInd Year; B.B.A. LL.B. (H)

Manasvi Ranjan

IInd Year; B.A. LL.B. (H)

Shreyamsi Brahma

IInd Year; B.A. LL.B. (H)

Anjana Nair

IInd Year; B.B.A. LL.B. (H)

Krishna Samith

IIIrd Year; B.A. LL.B. (H)

Anaaha Jaishankar

IIIrd Year; B.A. LL.B. (H)

Saakshi Mishra

IIIrd Year; B.B.A. LL.B. (H)

Dhruvi Shah

IIIrd Year; B.A. LL.B. (H)

Avishi Vats

IIIrd Year; B.A. LL.B. (H)

Nityashree Bhuvanaprasad

IIIrd Year; B.A. LL.B. (H)

TABLE OF CONTENTS

FROM THE DEAN'S DESK

I am honoured to present this latest edition of the *NMIMS Student Law Review*, marking another milestone in our journey of academic excellence. This edition is the result of extensive scholarly dedication and intellectual precision. Each article featured in this volume has undergone a rigorous peer-review process, ensuring that our publication upholds the highest standards of legal research and maintains an open, unbiased, and thought-provoking discourse.

This edition reflects the dynamic academic environment of the Kirit P. Mehta School of Law and the collective efforts of our institution to enrich legal scholarship. It covers a broad spectrum of contemporary legal issues, offering multiple perspectives on critical topics. By doing so, the *Review* serves as both a platform for knowledge dissemination and an intellectual space where legal theories are explored, debated, and refined. It is our hope that these discussions will not only deepen understanding but also inspire meaningful engagement with the evolving complexities of law and justice.

I extend my deepest gratitude to our esteemed Board of Advisors and Peer Reviewers, whose insights and guidance have been instrumental in shaping the depth and quality of this publication. Their expertise has helped transform this edition into a valuable scholarly resource, one that challenges existing legal frameworks while fostering innovative ideas.

A special acknowledgment goes to our dedicated Editorial Board, whose tireless efforts have played a crucial role in curating and refining the content of this journal. Their unwavering commitment to academic excellence and meticulous attention to detail deserve special recognition. Their passion for legal scholarship has ensured that each contribution is not only insightful but also meets the highest scholarly standards.

As you explore the pages of this edition, I encourage you to engage with the diverse analyses and perspectives presented.

Dr. Durgambini Patel

MENTOR'S MESSAGE

It is with great pride that I present this edition of the *NMIMS Student Law Review*, a reflection of our institution's commitment to legal scholarship. This volume brings together thought-provoking, peer-reviewed articles that showcase analytical depth and fresh perspectives on important legal issues. More than just a collection of insights, this journal encourages critical discussions and helps shape modern legal thinking.

At the Kirit P. Mehta School of Law, we emphasize both theoretical exploration and practical application of law. Through a blend of doctrinal analysis and real-world legal contexts, the *Review* amplifies emerging voices that challenge, refine, and redefine legal norms. The editorial team prioritized originality, strong methodology, and relevance to current legal debates. The selected articles not only engage with pressing legal issues but also provide practical insights for policymakers and practitioners. The dedication of the Editorial Board played a crucial role in refining these works. The peer-review process, combined with editorial discussions, ensured that only the most impactful contributions were published.

To our authors: your willingness to explore complex legal topics has enriched this journal's reputation. To our peer reviewers: your constructive critiques elevated the quality of each piece. We also extend our gratitude to our faculty advisors, whose guidance helped maintain the *Review's* alignment with global academic standards.

This edition is both a milestone and a promise—an achievement in legal scholarship and a step toward making legal knowledge more accessible. May these pages inspire readers to think critically about the law's evolving role in society and its power to drive positive change. Let us continue working together to innovate and uphold excellence in legal research for future generations.

Mr. Harshal Shah

ACKNOWLEDGMENT

Legal scholarship is an evolving dialogue—one that thrives on curiosity, critical thinking, and collaboration. The Seventh Edition of the *NMIMS Student Law Review* reflects this spirit, representing our academic community's shared goal of advancing legal discussions through thorough research and fresh perspectives. By pushing beyond traditional boundaries, this edition aims to set new standards in legal scholarship while honoring the dedication of everyone involved.

With a broader thematic focus and deeper analysis, this edition presents articles that challenge existing legal ideas while maintaining high academic standards. This publication would not have been possible without the guidance of Hon'ble Vice Chancellor, NMIMS University, and the leadership of Dr. Durgambini Patel, Dean of NMIMS Kirit P. Mehta School of Law, whose trust and support have shaped our editorial vision.

We sincerely thank our authors for their dedication to research and our Board of Peer Reviewers for their insightful feedback, ensuring the highest academic standards. The Registrar of NMIMS University, the administrative staff, and faculty members played a crucial role in facilitating this publication, providing the necessary support and mentorship to foster collaborative projects.

A special acknowledgment goes to our hardworking team: Student Head – Mr. Shashank Maheswari; Student Co-Head – Ms. Shubhangi Mishra; Student Editor-in-Chief – Mr. Dhruvit Shah; Student Co-Editor-in-Chief – Ms. Mahak Bhardwaj; Blogs Head – Ms. Chhavi Gupta; Editor-in-Chief (Blogs) – Ms. Aswathi Krishna; and the entire team of Content Editors. We also extend our heartfelt gratitude to our Mentor, Mr. Harshal Shah, whose guidance has been instrumental in maintaining the journal's academic quality.

As we present this edition, we celebrate not only its completion but also the collaborative spirit that drives academic progress. May this Review continue to inspire innovation and promote legal research that leads to meaningful societal change.

Prof. Richa Kashyap
Editor-in-Chief

FOREWORD

The Editorial Board is pleased to present the seventh volume of the NMIMS Student Law Review. With this edition, we continue our tradition of fostering meaningful legal discourse through the contributions of bright young legal minds.

Dhairya Jain, in *"Crypto Conundrum in Asia: Taxation, Regulation, and the Pursuit of Balance"*, explores the evolving landscape of cryptocurrency regulation across Asia. The article highlights the challenges governments face in integrating cryptocurrencies into traditional tax frameworks while balancing financial stability and investor protection. The study examines Japan's recognition of Bitcoin as legal tender to China's strict bans. Further, the paper delves into taxation complexities advocating for international cooperation and adaptive taxation policies.

Himanshu Chimaniya and Vishrut Veerendra, in *"Charting A Balanced Course: Safeguarding Consumer Rights In The Age Of AI Innovation"*, analyze the impact of AI on consumer rights, focusing on data collection, manipulation tactics, and liability concerns for AI-enabled products. The authors critique existing Indian and European consumer protection and product liability laws, arguing that they inadequately address AI-induced risks. They highlight gaps in data privacy laws, misleading contracts, and defective AI products, proposing regulatory reforms, and ex-ante approaches to mitigate potential harms caused by AI-driven decision-making systems.

Aanchal Agarwal and Kuhu Srivastava, in *"Hyper-Personalization in Insurance Vis-à-Vis Data Privacy"*, examine the rising trend of hyper-personalization in the insurance sector, where AI and big data analytics enable tailored policies and pricing based on individual consumer data. The authors assert that these advancements pose significant data privacy risks, raising concerns about informed consent, data security, and potential discrimination. The paper critiques existing data protection laws and suggests a need for stricter regulations to balance innovation with consumer rights, ensuring ethical AI deployment in the insurance industry.

We extend our heartfelt congratulations to the authors and express our gratitude to our dedicated team of editors for their relentless commitment, perseverance, and dedication to promoting outstanding legal scholarship. Their unwavering efforts have been crucial in bringing forth insightful and high-quality legal literature of the highest standard.

Board of Editors

Short Article

CRYPTO CONUNDRUM IN ASIA: TAXATION, REGULATION, AND THE PURSUIT OF BALANCE

- DHAIRYA JAIN

ABSTRACT

The rise of cryptocurrencies and blockchain technology has ushered in a new era of financial innovation and technological advancement. Policymakers are currently contending with the challenge of incorporating cryptocurrencies into tax systems that were not originally structured to accommodate such assets. Regulators are confronted with a formidable challenge as they strive to identify and find a harmonious equilibrium between fostering innovation on one hand and ensuring financial stability and safeguarding investor interests on the other. This analytical article delves into the intricate web of tax complexities that surround cryptocurrencies and blockchain technology across various Asian economies. Through Japan's recognition of Bitcoin as a legal tender, China's stringent crypto bans, and Singapore's attempt to provide clarity through specific guidance to India's oscillation between prohibition and acceptance, the article examines the diverse strategies Asian nations employ. The decentralized nature of blockchain technology, coupled with cross-border transactions and anonymity features, presents unique challenges in accurately assessing and collecting taxes. The borderless nature of cryptocurrencies and the global accessibility of blockchain networks raise questions about jurisdictional authority and information sharing between countries. The article explores how this aspect adds complexity to enforcing tax compliance and preventing tax evasion.

Keywords*:* Cryptocurrencies Blockchain, Innovation Regulatory challenges, Tax complexities.

I. INTRODUCTION

The financial environment is subject to continuous change, characterised by ongoing advancements in distribution channels, as well as the introduction of new products and services. Digitalization is a prominent and influential trend that has brought about significant transformations in the manner in which consumers and investors engage with conventional financial products and services.

One such innovation that has caught the attention of the public and policymakers throughout the world in recent times is Virtual Digital Assets ("**VDAs**"). The remarkable growth of cryptocurrencies and blockchain technology represents a milestone where finance and technology intersect. This rapid rise has sparked a wave of creativity and change fundamentally reshaping the landscape. However, this transformation has not been without its obstacles. Policymakers and regulators are facing the challenge of incorporating cryptocurrencies into tax systems[1] which were not initially designed to handle these assets. Finding the equilibrium, between promoting innovation, maintaining stability, and protecting investor welfare has become an utmost priority.

Due to the explosive development of cryptocurrencies and the game-changing blockchain technology, Asia has become a global Crypto-developer powerhouse.[2] As a result, the financial industry is now experiencing an era of unprecedented innovation and growth. The proliferation of VDAs has confronted policymakers and regulators with a plethora of nuanced new issues. They must find a way to tax these assets inside frameworks designed for more traditional sources of wealth. To incorporate innovations in the usage of crypto assets into a well-functioning tax

---

[1] Baer, K. *et al. Crypto poses significant tax problems-and they could get worse*. INTERNATIONAL MONETARY FUND (Jan. 12, 2025), https://www.imf.org/en/Blogs/Articles/2023/07/05/crypto-poses-significant-tax-problems-and-they-could-get-worse.

[2] Adejumo, O. *Asia emerges as new crypto developer powerhouse, leaving us behind*, CRYPTOSLATE. (Jan. 13, 2025), https://cryptoslate.com/asia-emerges-as-new-crypto-developer-powerhouse-leaving-us-behind

system is the first order of challenges for tax authorities. Whether cryptocurrencies die out or thrive, the tax system will still have to account for them.

II. UNDERSTANDING VDAS, BLOCKCHAIN AND CRYPTOCURRENCIES

In the ever-changing digitised world of the present times, a whole new class of assets called Virtual Digital Assets has emerged which has changed the way how we think of money, ownership, and value. VDAs are digital representations of value, stored electronically and capable of being traded, transferred, or used as a medium of exchange.[3] Although digital currencies like Bitcoin and Ethereum are the most popular examples of VDAs, the category also encompasses other digital tokens and collectables, including Non-Fungible Tokens. What makes these assets so appealing is that they exist only in the digital space; thus, anyone in the world can buy, sell, or trade them without their physical forms and interference from any middlemen, like banks or governments.

The mainstay for many VDAs, in particular cryptocurrencies, is revolutionary technology called Blockchain. In simple words, Blockchain is a virtual ledger – a system to record transactions.[4] Unlike what happens in traditional systems where an intermediary entity usually a bank maintains a record of transactions, blockchain is decentralised. This essentially means that the digital ledger is scattered in a network of computers to make sure that no one controls the information. Every transaction is recorded in a "block," and these are then connected in one long chain, hence the name "blockchain."[5] The genius lies in this: once added, a block can never be changed or deleted, thus providing an immutable and transparent record. This also makes blockchain an attractive feature of cryptocurrencies, whereby any transaction

---

[3] Sheldon, R., *What is a virtual asset and how does it work?*, TECHTARGET. (Jan. 13, 2025), https://www.techtarget.com/whatis/definition/virtual-asset

[4] *What is blockchain? - blockchain technology explained* – AWS. (Jan. 13, 2025), https://aws.amazon.com/what-is/blockchain/

[5] *What is blockchain? IBM*. (Jan. 13, 2025), https://www.ibm.com/topics/blockchain

involved in it is secure and verifiable by all parties concerned and without the need for involvement by any third party.

Cryptocurrencies are digital forms of money which run on blockchain technology and are among the most visible applications of VDAs.[6] Cryptocurrencies, such as Bitcoin, allow value to be directly transferred from one owner to another, dispensing with the need for intervention by banks or any other intermediaries. All transactions are recorded on a blockchain securely and transparently. What is unique about cryptocurrencies is that they are independent of any central authorities like governments or financial institutions. By the same virtue, this decentralization can make transactions quicker, more affordable, and accessible on a global level. However, cryptocurrency values can also be quite volatile, meaning the value may see extreme highs and lows in very short intervals. In addition, their anonymity and lack of control by a single central authority raise concerns about criminal uses and result in increased demands for greater regulations and scrutiny.

While blockchain technology and cryptocurrencies are changing the way we think about finance, it is much more than that; blockchain technologies have a wide field of application. The above-mentioned industries garner an immutable record of transactions within the blockchain, allowing for a high degree of data integrity and making fraudulence or manipulation all but impossible. Notwithstanding, this promise about blockchain and VDAs, challenges are there to be sorted out. Problems of scalability, consumption of energy-especially in such cryptocurrencies like Bitcoin that require immense loads of it[7] and questions related to the legality of ownership and their taxes are active explorations both from regulators and technologists.

---

[6] *What is cryptocurrency and how does it work?* KASPERSKY. (Jan. 13, 2025) https://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency

[7] Huestis, S. *Cryptocurrency's Energy Consumption Problem*, *RMI*. (Jan. 13, 2025) https://rmi.org/cryptocurrencys-energy-consumption-problem

III. THE CRYPTOCURRENCY LANDSCAPE IN ASIA

Cryptocurrencies and the blockchain technology upon which they are built have proliferated since Bitcoin's introduction in 2008, a watershed point in the history of the global financial system. In recent years, Asia has emerged as the predominant hub for the acceptance of cryptocurrencies, significant trading volumes, and the experimental development of blockchain applications.[8] The wide range of regulatory measures seen in Asian nations such as China's strict crypto restrictions, Japan's acceptance of Bitcoin as legal currency, Singapore's targeted regulations, and South Korea's regulation of crypto trading highlights the complex landscape of potential and regulatory challenges brought forth by virtual technology. In the future, it is quite likely that collaborative efforts among Asian governments will play a crucial role in building global normative frameworks that control the rising trajectory of cryptocurrencies and decentralised networks. The implementation of this collaborative imperative can determine the course of this swiftly evolving landscape worldwide.

The concentration of trading volumes in the Asian region persists, mostly due to the significant presence of large exchanges like Binance and Upbit, accounting for over 35% of global daily cryptocurrency trade volumes.[9] Japan has been a leading example in the retail sector, as it has seen widespread implementation of cryptocurrencies for various forms of payment. Respected business institutions, such as Marui Department Stores[10], Bic Camera[11], and Mercari[12], have initiated exploring endeavours in a range

---

[8] Jahan, *et al. Towards central bank digital currencies in Asia and the Pacific: Results of a regional survey*, *IMF eLIBRARY*. (Jan. 13, 2025) https://doi.org/10.5089/9798400221521.063

[9] *Market Share of Centralized Crypto Exchanges COINGECKO*. (Feb. 18, 2025) https://www.coingecko.com/research/publications/centralized-crypto-exchanges-market-share

[10] *Japanese department store begins trialing Bitcoin payments*, COINGEEK. (Jan. 13, 2025), https://coingeek.com/japanese-department-store-begins-trialing-bitcoin-payments

[11] *Japanese consumer electronics retailer opens up to Universal Bitcoin payments*. COINGEEK. (Jan. 13, 2025), https://coingeek.com/japanese-consumer-electronics-retailer-opens-universal-bitcoin-payments

[12] Jha, P. *Japanese e-commerce giant Mercari to allow Bitcoin payments from June*, *COIN TELEGRAPH* (Jan. 13, 2025), https://cointelegraph.com/news/japanese-e-commerce-giant-mercari-allow-bitcoin-payments-june

of blockchain and cryptocurrency applications, indicating a growing acknowledgement of the many possibilities offered by this technology. However, using cryptocurrencies for everyday transactions is still in its early stages[13], as authorities carefully manage the balance between promoting innovation and managing associated dangers. The adoption of remittances and investing activities remains significant among scattered communities and digitally-native populations.

Countries like Singapore, Japan, and South Korea have proactively fostered hubs of innovation focused on the development and use of blockchain technology. These enclaves function as catalysts for a wide range of initiatives that include financial applications, tracking the origin and history of assets, coordinating supply chains, and developing solutions for digital identification. Furthermore, several technical communities in Asia actively participate in collaborative initiatives that include a wide range of blockchain platforms, including well-established ones like Ethereum and emerging platforms such as Polkadot.[14] Asia is seen as a dynamic terrain that serves as an experimental furnace for emerging crypto-business ideas.

Governments in many Asian countries have contrasting viewpoints, which include restrictions on crypto mining as well as the formulation of entire national initiatives pertaining to blockchain technology. Regulatory authorities are faced with the complex problem of reconciling the demands of facilitating innovation while also adhering to Anti-Money Laundering ("**AML**") regulations and considering the potential risks to financial stability.

---

[13] Kortam, R. (2022) *Cryptocurrencies can improve speed, cost and ease of access of payments*, *OMFIF*. (Jan. 13, 2025) https://www.omfif.org/2023/01/cryptocurrencies-can-improve-speed-cost-and-ease-of-access-of-payments/

[14] *Key local blockchain communities pushing for adoption in the Philippines.* COINGENIUS. https://coingenius.news/key-local-blockchain-communities-pushing-for-adoption-in-the-philippines-bitpinas/ (Jan. 13, 2025).

IV. TAXATION CHALLENGES POSED BY CRYPTOCURRENCIES

The emergence of cryptocurrencies has presented novel problems to conventional tax frameworks on a global scale. Governments are now faced with the challenge of successfully imposing taxes on VDA transactions and guaranteeing adherence to tax regulations, as the popularity and utilisation of these assets continue to grow.

A. Traditional Tax Systems vs. VDAs

i. Understanding Traditional Tax Systems

The development of traditional tax systems has occurred gradually over an extended period, spanning several centuries, with the primary objective of effectively governing and overseeing economic activity inside a given nation. Centralised organisations such as banks, government agencies, and tax authorities are relied upon for revenue collection. The use of a centralised strategy facilitates the process of monitoring and documenting taxable activities in a reasonably simple manner. A range of tax categories are used, including income tax, capital gains tax, property tax, as well as consumption taxes such as value-added tax ("**VAT**"), or sales tax. These systems have been widely recognised and provide explicit protocols to report and ensure adherence to regulations. Income tax encompasses earnings, which stem from virtual asset transactions; capital gains tax covers those derived from their sale; VAT/GST allows commercial transactions to generate revenue. Withholding tax is levied right at the creation of revenue, transaction tax deals with frequently traded items, and inheritance tax covers the case of transfer of wealth. Taken together, these taxes promote transparency, prevent evasion, and make the virtual asset ecosystem pay its fair share towards the overall tax base.

ii. Lack of Visibility and Reporting

Tax authorities have a significant issue in effectively taxing cryptocurrencies due to the dearth of visibility and transparency. In contrast to conventional financial systems,

which rely on centralised entities such as banks for conducting transactions, these transactions are conducted in a peer-to-peer manner, and while the blockchain records the transaction information, they are not necessarily associated with particular persons. The limited visibility in this context is a notable obstacle for tax authorities, who depend on specialised methodologies and technologies to track and authenticate taxable transactions. Although the specifics of these transactions are recorded on the publicly accessible ledger, they are not fundamentally associated with tangible identities in the physical world. The presence of intrinsic anonymity and pseudonymity inside crypto transactions poses a challenge for tax authorities in effectively tracking and verifying taxable activity. Fundamentally, tax authorities face a disparity in their ability to observe crypto transactions compared to conventional bank transactions. Due to the pseudonymous characteristics inherent in crypto transactions, tax authorities often have challenges in establishing direct associations between certain transactions and identifiable persons or companies.

iii. Valuation Challenges

The valuation of cryptocurrencies is a very unique challenge, quite different from traditional assets, both tangible and intangible. While traditional assets, such as real estate or stocks, can effectively be valued based on clear and more measurable factors like location and size, company performance, or market price, respectively, cryptocurrencies are highly resistant to conventional valuation methods due to their intangible and highly volatile nature.

On the other hand, unlike traditional intangibles, such as IPR, which can be appraised given their capacity to yield revenues, demand conditions in markets, and even legality of rights granted, cryptocurrencies are bereft of any substantial asset-or, at least, a tangible claim-which provides the backdrop of valuation. In the case of a patent, its value could be decided using efficiency or its capacity to generate a constant stream of royalty incomes. Its value would again be reflected based on the

identification of that trademark. These assets are intangible but tied to measurable and predictable outcomes. Cryptocurrencies are not linked to any form of physical or business-backed asset, and most of the value comes from speculative elements, market demand, and investor psychology.

This, of course, is further exacerbated by a basic lack of any widely accepted pricing mechanism for cryptocurrencies. Whereas stocks are normally traded on centralized exchanges with uniform pricing, cryptocurrencies are decentralized and traded on a multitude of platforms-many times resulting in price discrepancies between exchanges.[15] Further, unlike tangible assets like real estate that may have specific appraisals in respect of physical attributes, or IPR that can be appraised with their respective earnings potential, there is nothing concrete on which any value for virtual currencies could be based. The price mainly depends on exogenous factors like investor appetite, technological development, and the global regulatory environment. This, in return, makes the gap huge when trying to apply traditional valuation models to cryptocurrencies, because the factors that influence their worth are most often unpredictable and fluctuating[16].

B. Unique Challenges Presented by Decentralization and Anonymity

i. Decentralization and its Impact on Taxation

The influence of decentralisation on taxes is a significant aspect to consider since the decentralised nature of cryptocurrencies fundamentally transforms the conventional taxation framework. In traditional financial frameworks, tax authorities may depend on centralised institutions and regulatory agencies to supervise and implement tax regulations. In contrast, cryptocurrencies function on decentralised blockchain

---

[15] Milne, J. and Bradine, C. *Cryptocurrency: The next chapter in the valuation conundrum*. CONYERS (Jan. 14, 2025), https://www.conyers.com/publications/view/cryptocurrency-the-next-chapter-in-the-valuation-conundrum/

[16] *What affects Crypto's price? Crypto volatility*. FIDELITY. (Jan. 14, 2025), https://www.fidelity.com/learning-center/trading-investing/bitcoin-price

networks, which lack a central authority or mediator. The absence of a centralised governing authority presents substantial challenges for the enforcement of taxation.[17] In contrast to conventional systems, where organisations may be subject to regulation and oversight, the decentralised nature of cryptocurrencies presents challenges in identifying and locating taxpayers involved in crypto transactions. Tax authorities need to adjust to this emerging paradigm by formulating inventive approaches that are in line with the decentralised characteristics of VDAs. This may include using sophisticated technology, such as blockchain analytics to acquire discernment into transactional operations without depending on centralised institutions.

ii. Anonymity and its Implications for Taxation

The concept of anonymity and its ramifications about taxation: The use of pseudonyms in blockchain transactions has a two-fold impact on the effectiveness of tax enforcement endeavours. On the one hand, cryptocurrencies provide users with a certain level of anonymity and security, which is a highly sought-after characteristic. Nevertheless, the presence of anonymity poses significant obstacles for tax officials. Cryptocurrency transactions are documented on a publicly accessible ledger using cryptographic addresses instead of human identification. Although the transactional information is visible, the identity of the persons involved remains undisclosed. The task of tax authorities in establishing a direct connection between certain transactions and real-world persons or companies presents a substantial problem. Consequently, the task of confirming taxable activity and enforcing tax obligations becomes intrinsically challenging. Furthermore, the presence of anonymity in cryptocurrency transactions poses a potential threat of tax evasion, as individuals may seek to hide their identities or provide inaccurate information on their crypto assets to avoid fulfilling their tax obligations.

---

[17] Avalos, S. *Challenges that Cryptoasset anonymity creates for Tax Administration*. JOURNAL OF TAX ADMINISTRATION. (Jan. 14, 2025), https://www.jota.website/jota/article/view/165

iii. Tracking and Monitoring Challenges

Challenges in the tracking and monitoring of cryptocurrencies arise due to their decentralised and anonymous character, which significantly increases the intricacy involved in identifying and overseeing taxable transactions. In conventional financial frameworks, tax authorities acquire transaction data from banks or financial organisations in order to streamline tax enforcement processes[18]. Nevertheless, the standard methodology is not suitable inside the realm of cryptocurrencies. In order to efficiently detect and monitor taxable actions, it is essential for tax authorities to allocate resources towards the acquisition of specialised tools and technology, including blockchain analytics. The use of sophisticated technologies allows tax authorities to effectively manage the intricate nature of blockchain technology and derive significant insights from transactional data. Through the use of these technologies, tax authorities may augment their capacity to oversee and enforce tax legislation within the ever-changing and dynamic realm of digital finance.

The distinct difficulties arising from decentralisation and anonymity in the context of cryptocurrencies taxes need tax authorities to adopt new approaches and instruments. In order to successfully negotiate and enforce tax regulations inside the cryptocurrency ecosystem, tax authorities must undertake crucial measures such as adapting to the decentralised nature of VDAs, resolving the complications associated with anonymity, and investing in sophisticated technology.

C. Jurisdictional Issues and Cross-Border Transactions

The presence of jurisdictional challenges and the role of cryptocurrencies in enabling cross-border transactions contribute to the intricacies of taxes. The inherent global character of cryptocurrencies presents a significant challenge in effectively

[18] Baer, K. *et al. Crypto poses significant tax problems-and they could get worse*, *IMF*. (Jan. 14, 2025), https://www.imf.org/en/Blogs/Articles/2023/07/05/crypto-poses-significant-tax-problems-and-they-could-get-worse

implementing tax legislation across international boundaries. In contrast to conventional assets or transactions, which are normally limited to a certain state, cryptocurrencies can transcend national boundaries rapidly. The aforementioned issue poses a substantial challenge for tax authorities in their endeavour to enforce their national tax legislation on these fundamentally boundary-less VDAs.

i. Complexity of Cross-Border Transactions

Cryptocurrencies' ability to promote international trade without the need for centralised financial institutions marks a significant change in the world of international finance. This capability facilitates the speedy and trouble-free completion of cross-border transactions by both people and businesses. While undoubtedly impressive, this development poses a serious problem for tax collectors. Most transactions in traditional financial systems follow well-established banking routes, making it easy for tax authorities to monitor and control them.[19] Cryptocurrencies, on the other hand, function on decentralised networks that eliminate the middlemen. Because of the inherent difficulty in determining the proper jurisdiction for taxes, this decentralisation poses serious problems for the traditional paradigm of cross-border financial transactions. Another factor adding complexity is the lack of a single body responsible for monitoring these exchanges. Finance agencies are struggling to determine who has the right to regulate and tax cryptocurrency transactions across borders. Given the fundamentally global character of cryptocurrencies, it is clear that implementing tax legislation on international crypto transactions would be a significant difficulty.

---

[19] Baer, K. *et al*. *IMF Working paper on Taxing Crypto Currencies*, *IMF*. (Jan. 14, 2025), https://www.imf.org/-/media/Files/Publications/WP/2023/English/wpiea2023144-print-pdf.ashx

ii. Lack of International Standards

The complexity of taxes is further exacerbated by the lack of globally acknowledged and standardised international tax legislation that is expressly designed for cryptocurrencies. Every country has its specific collection of tax rules and regulations, which are influenced by its own economic and legal frameworks.[20] The existence of many tax systems results in considerable variation in the taxation of cryptocurrencies across different jurisdictions. Different governments may classify cryptocurrencies in various ways, with some seeing them as commodities, while others perceive them as currencies or assets. The absence of consistency gives rise to a multifaceted environment in which the tax consequences of cryptocurrency transactions might significantly differ depending on the geographical jurisdiction. The danger of double taxation is heightened by the possibility of divergent tax regimes across many jurisdictions, whereby the same income or transaction may be subjected to taxes in numerous nations. The lack of alignment between different parties involved in cross-border cryptocurrency transactions not only creates practical difficulties but also provides considerable obstacles for tax authorities aiming to implement fair and uniform tax regulations. The task of attaining worldwide tax cooperation and consistency presents a significant obstacle, as it necessitates negotiating the intricate landscape of many legal and economic frameworks.

iii. International Cooperation and Information Sharing

The successful resolution of tax issues associated with cryptocurrencies requires a significant level of international collaboration and the exchange of information among tax authorities. Collaboration plays a crucial role in the establishment of shared standards, the exchange of critical information, and the precise enforcement of tax legislation. Nevertheless, attaining such a degree of collaboration presents itself as a

[20] *International standards on tax transparency*. OECD. (Jan. 14, 2025), https://www.oecd.org/en/topics/sub-issues/international-standards-on-tax-transparency.html

multifaceted undertaking. The existence of divergent national agendas, legal frameworks, and economic interests have the potential to hinder the advancement of coordinated tax policy.[21]

In contrast to conventional financial systems, which rely on centralised institutions to allow the flow of information, cryptocurrencies function on decentralised networks that run without a single authority supervising transactions. The need for decentralisation necessitates the development of novel strategies for the dissemination of information and the coordination of activities among tax authorities. Addressing these problems necessitates a collaborative endeavour to reconcile divergent viewpoints and establish a consensus about the taxation of cryptocurrencies within an integrated global economy.

V. POLICY RESPONSES ACROSS ASIAN ECONOMIES

A. Japan: Recognition of Bitcoin as a Legal Tender

Japan has emerged as the leader in cryptocurrency regulation, starting with recognising Bitcoin and other virtual assets as valid forms of property according to the Payment Services Act ("**PSA**") in April 2017. Subsequently, the nation has consistently revised and enhanced its regulatory framework.[22]

In May 2020, Japan made significant changes by amending the PSA and the Financial Instruments and Exchange Act ("**FIEA**") to replace the term 'virtual currency' with 'crypto-asset.' The objective of this modification was to establish more precise directives for bitcoin exchanges and trading platforms.[23]

---

[21] *International standards for Automatic Exchange of information in Tax Matters.* OECD. (Jan. 14, 2025) https://www.oecd.org/en/publications/2023/06/international-standards-for-automatic-exchange-of-information-in-tax-matters_ab3a23bc.html

[22] *Crypto regulations in Japan*. COMPLY ADVANTAGE. (Jan. 14, 2025) https://complyadvantage.com/insights/cryptocurrency-regulations-around-world/cryptocurrency-regulations-japan/

[23] *Japan's new crypto regulation.* HUB | K&L GATES. (Jan. 14, 2025) https://www.klgates.com/Japans-New-Crypto-Regulation-2019-Amendments-to-Payment-Services-Act-and-Financial-Instruments-and-Exchange-Act-of-Japan-11-26-2019

According to the provisions of the Public Service Announcement ("**PSA**"), cryptocurrency exchanges are required to undergo registration with the Financial Services Agency ("**FSA**") and comply with regulations pertaining to anti-money laundering and counter-terrorism financing ("**AML/CFT**"). These measures are implemented to guarantee transparency and enhance the security of investments for individuals involved in cryptocurrency transactions.

In addition, it is worth noting that the National Tax Agency classifies gains from cryptocurrencies as "miscellaneous income," making purchasers liable for taxation.

In response to the issues presented by decentralised cryptocurrencies and the associated concerns of money laundering, Japan implemented the Act on Prevention of Transfer of Criminal Proceeds ("**APTCP**"). The aforementioned legislation mandates the implementation of AML regulations for Virtual Asset Service Providers ("**VASPs**"), imposing upon them the responsibility to conduct rigorous Know-Your-Customer ("**KYC**") verifications and retain transaction documentation for a period of seven years.[24]

Furthermore, Japan's regulatory landscape has also acclimated to international standards established by the Financial Action Task Force ("**FATF**"), requiring crypto asset businesses to implement anti-money laundering and counter-terrorism financing measures.

B. China: Stringent Regulations and Crypto Bans

The Chinese cryptocurrency market holds a prominent position globally, thereby exerting a significant influence on the fluctuations of cryptocurrency prices worldwide. The nation enforces the most stringent regulatory measures with regard to cryptocurrency[25]. The current regulatory measures encompass a comprehensive

---

[24] *AML/CFT/CPF in Japan*. MINISTRY OF FINANCE. (Jan. 14, 2025) https://www.mof.go.jp/english/policy/international_policy/amlcftcpf/3.efforts.html

[25] *What's behind China's cryptocurrency ban?* WORLD ECONOMIC FORUM. (Jan. 14, 2025), https://www.weforum.org/stories/2022/01/what-s-behind-china-s-cryptocurrency-ban/

prohibition on all activities associated with cryptocurrencies, thereby prohibiting companies from engaging in any form of cryptocurrency services, including mining, trading, and the issuance of cryptocurrencies.

The Provisions on the Administration of Blockchain Information Services, which are overseen by the Cyberspace Administration of China, regulate China's internet and specifically govern blockchain information services. Blockchain-related services are also subject to the Encryption Law of the People's Republic of China, which governs encryption productions and standards.[26] The People's Bank of China, the Ministry of Industry and Information Technology, the China Banking Regulatory Commission, the China Securities Regulatory Commission, and the China Insurance Regulatory Commission issued the "Notice on Preventing Bitcoin Risks" (Notice) on 3rd December, 2013. On 4th September, 2017, seven ministries published: "Announcement on Preventing Token Issuance Financing Risks" (Announcement). [27]

Bitcoin is not a legal tender. Both the "Notice" and the "Announcement" emphasise that Bitcoin lacks the characteristics of a traditional currency, as it is not issued by a monetary authority, lacks monetary properties such as legal tender and enforceability, does not possess the same legal standing as a recognised currency, and should not be utilised as a medium of exchange in the market.

The state prohibits some Bitcoin-related activities, which include trading platforms being barred from facilitating the exchange of legal cash and tokens, as well as being restricted from buying or selling tokens as a central counterparty. Financial institutions and non-bank payment institutions are prohibited from engaging in the direct or indirect provision of goods or services linked to token issuance. This includes activities like account opening, registration, trading, clearing, and settlement.

[26]*Cryptography Law of the P.R.C.* CHINA LAW TRANSLATE. (Jan. 14, 2025), https://www.chinalawtranslate.com/en/cryptography-law

[27]*China and cryptocurrency*. FREEMAN LAW. (Jan 14., 2025), https://freemanlaw.com/cryptocurrency/china

Additionally, these institutions are not permitted to underwrite tokens associated with such activities.

The state does not impose restrictions on Bitcoin's operations as virtual commodities, with the exception of instances when Bitcoin is used as a recognised form of legal money.

In May 2021, the Financial Stability and Development Committee of China, functioning under the leadership of Vice-Premier Liu He, declared the Chinese government's intention to implement stringent restrictions targeting bitcoin mining and trading operations. The primary objective of the government was to effectively discourage the shifting of personal risks onto the broader societal framework.[28] This announcement led to a significant decline in bitcoin's value, with the cryptocurrency experiencing a notable drop in its market price. [29]

Nonetheless, recent reports indicate that the Chinese government is contemplating a change in its stance. The motivation behind this potential reversal is multifaceted. China recognises the increasing global interest in and adoption of cryptocurrencies, and it aims to capitalize on the potential economic advantages and technological advancements that blockchain technology offers.

Furthermore, China has been actively exploring the development of its own central bank digital currency ("**CBDC**"), known as the digital yuan or e-CNY. By lifting the cryptocurrency ban, China could create a more favourable environment for the adoption of its CBDC, enabling it to compete with established cryptocurrencies like Bitcoin and Ethereum.[30]

---

[28] *China doubles down efforts on virtual currency regulation*. THE STATE COUNCIL OF P.R.C. (Jan. 14, 2025) https://english.www.gov.cn/news/topnews/202105/25/content_WS60ac3689c6d0df57f98da07f.html

[29] *Bitcoin ends day on the ropes after China clamps down on mining, trading*. REUTERS. (Jan. 14, 2025) https://www.reuters.com/technology/bitcoin-under-pressure-comeback-fades-2021-05-21/

[30] *China is combating crypto with a push for the Digital Yuan*. QUARTZ. (Jan. 14, 2025). https://qz.com/2065913/chinas-answer-to-crypto-is-the-digital-yuan

C. Singapore: Clarity Through Specific Guidance

Since June 2013, the Monetary Authority of Singapore ("**MAS**") has issued warnings to both consumers and companies about the significant risks connected with virtual currency transactions[31]. In August 2017, MAS provided clarification regarding the initial coin offering ("**ICO**") in response to the significant increase in ICO activity observed in 2016. MAS emphasised that ICOs must comply with the prevailing securities regulations, which are in place to safeguard the interests of investors, particularly in cases when tokens exhibit characteristics similar to securities. On August 10, 2017, the Monetary Authority of Singapore MAS and the Commercial Affairs Department released a joint warning. In this advisory, MAS highlighted the importance for consumers to exercise caution and thorough understanding when it comes to the possible risks associated with ICOs and investment schemes that use digital tokens.[32]

However, in that particular timeframe, MAS explicitly stated its intention to regulate virtual currency intermediaries in Singapore as a means to address the possible concerns associated with money laundering and terrorist funding. It should be noted that MAS did not express any intentions to directly control virtual currencies themselves.

In December 2017, concurrent with the substantial increase in the value of Bitcoin, reaching approximately US$20,000 in December 2017, compared to a mere US$1,000 in January 2017[33], and the subsequent surge in interest towards cryptocurrency investments, MAS reiterated the importance for individuals to exercise extreme

---

[31] *Singapore regulates virtual currencies to combat money laundering and terrorism.* PINSENT MASONS. (Jan. 14, 2025). https://www.pinsentmasons.com/out-law/news/singapore-regulates-virtual-currencies-to-combat-money-laundering-and-terrorism

[32] *Consumer Advisory on Investment Schemes Involving Digital Tokens*. MONETARY AUTHORITY OF SINGAPORE. (Jan. 14, 2025). https://www.mas.gov.sg/news/media-releases/2017/consumer-advisory-on-investment-schemes-involving-digital-tokens

[33] *Bitcoin price in 2017* BITBO CALENDAR. (Jan. 14, 2025). https://calendar.bitbo.io/price/2017

caution and possess a comprehensive understanding of the substantial risks associated with such investments.

The MAS issued a cautionary statement highlighting that the notable increase in cryptocurrency values can be attributed to speculative activities, hence posing a considerable risk of significant price fluctuations. Furthermore, MAS underscored the lack of regulatory safeguards in place to protect investments in cryptocurrencies.

In January 2022, MAS implemented regulatory measures aimed at limiting the promotion and advertisement of cryptocurrency services in public domains, as well as discouraging the portrayal of cryptocurrency trading in a manner that underestimates its associated dangers.[34]

On 26th October, 2022, approximately two weeks prior to the bankruptcy filing of FTX on 11th November, 2022, MAS released two consultation papers. These papers outlined suggested measures aimed at reducing the potential harm to consumers engaged in cryptocurrency trading, as well as promoting the development of stablecoins within Singapore's VDA ecosystem. The first paper was titled "Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services,[35]" while the second paper was titled "Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities."[36]

---

[34] *Consultation Paper on Proposed Regulatory Measures For Digital Payment Token Services.* MONETARY AUTHORITY OF SINGAPORE. (Jan. 14, 2025). https://www.mas.gov.sg/-/media/mas/news-and-publications/consultation-papers/2022-proposed-regulatory-measures-for-dpt-services/annexes-part-2.pdf

[35] *Consultation Paper on Proposed Regulatory Measures for Digital Payment Token Services* MONETARY AUTHORITY OF SINGAPORE. (Jan. 14, 2025). https://www.mas.gov.sg/publications/consultations/2022/consultation-paper-on-proposed-regulatory-measures-for-digital-payment-token-services

[36] *Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities*. MONETARY AUTHORITY OF SINGAPORE. (Jan. 14, 2025). https://www.mas.gov.sg/publications/consultations/2022/consultation-paper-on-proposed-regulatory-approach-for-stablecoin-related-activities

D. South Korea: Implementation of Real-Name Trading Accounts

In the year 2017, the South Korean government implemented steps aimed at restricting the usage of anonymous accounts in cryptocurrency trading. Additionally, they imposed a prohibition on local financial institutions from assisting Bitcoin futures transactions, thereby indicating a possible inclination towards a ban. In 2018, the Financial Services Commission (**"FSC**") implemented augmented reporting obligations for banks that have crypto exchange accounts.[37]

According to the Virtual Asset Real-Name Account Operation Guidelines, the trading of cryptocurrencies is now restricted to "real-name bank accounts." This implies that individuals engaging in cryptocurrency trading must establish a bank account under their legal name with the same financial institution as their chosen cryptocurrency exchange. This requirement enables them to deposit or withdraw funds from their electronic wallets. Both financial institutions, namely the bank and the exchange, are required to comply with established AML/CFT regulations and structured transaction reporting obligations.

In the year 2020, the government of South Korea revised current legislation intending to expand the scope of mandatory AML/CFT duties to encompass all domestic trades. By the end of September 2021, businesses were required to obtain a licence from the Financial Intelligence Unit of the Financial Services Commission to operate. Due to the implementation of recent cryptocurrency rules, it became mandatory for all providers of cryptocurrency services to enhance AML and KYC systems, as well as undergo registration with financial regulatory bodies in Korea, prior to initiating their business.[38]

---

[37] *Financial Measures to Curb Speculation in Cryptocurrency Trading*. FINANCIAL SERVICES COMMISSION. (Jan. 14, 2025) https://www.fsc.go.kr/eng/pr010101/22173

[38] *The new crypto regulations in South Korea: How to prepare for the changes.* SUMSUB. (Jan. 14, 2025). https://sumsub.com/blog/crypto-regulations-south-korea

The aforementioned laws are an extension of the measures implemented by the FSC in 2018. These regulations now require a wide variety of virtual asset service providers to adhere to AML/CFT requirements as mandated by South Korean legislation. These actions attempt to promote a safer financial environment by giving financial regulators access to bitcoin transaction data.

E. India: Oscillation between Prohibition and Acceptance

India's stance towards cryptocurrencies and blockchain technology has been characterised by a sequence of fluctuations, alternating between periods of complete restriction and cautious acknowledgement. The aforementioned ambivalence is indicative of the intricate problems and prospects that these technologies provide to the Indian economy and regulatory framework.

During the first phase of bitcoin adoption, regulatory agencies in India followed a cautious approach. The Reserve Bank of India (**"RBI"**) has issued a series of cautionary statements to the general public on the potential hazards linked to the practice of trading and investing in cryptocurrencies. During this particular time frame, there was a restricted level of regulatory lucidity, with the primary emphasis of Indian authorities being on the issuance of advice.

In April 2018, a notable transformation occurred in the regulatory framework when the RBI implemented a prohibition on transactions pertaining to cryptocurrencies inside the banking sector.[39] This measure essentially imposed a prohibition on banks and financial organisations from offering their services to bitcoin exchanges and dealers. The imposition of the ban resulted in a notable upheaval within the cryptocurrency ecosystem in India, compelling some exchanges to cease operations or transfer their activities elsewhere.

---

[39] *Regulating cryptocurrency in India*. INTERNATIONAL BAR ASSOCIATION. (Jan. 14, 2025) https://www.ibanet.org/article/2e4fb646-4ffd-4660-a5be-5e41e79c5576

In March 2020, the Sup. Ct. of India made a significant ruling by lifting the banking ban imposed by the RBI on cryptocurrencies. The aforementioned ruling was a significant turning point for the cryptocurrency business in India, as it offered a renewed opportunity for exchanges and dealers.[40] Subsequently, there has been an increasing acknowledgement of the potential advantages offered by blockchain technology, and deliberations pertaining to the development of a complete legislative framework have gained traction.

In 2021, there were rumours surfaced suggesting that the Indian government was contemplating the implementation of a preliminary legislation that outlined a complete structure for the governance of cryptocurrencies. The proposed legislation purportedly aimed to provide clear definitions and regulatory measures for digital currencies, possibly enabling the development of a central bank digital currency (**"CBDC"**) while implementing limitations on privately issued cryptocurrencies.

As of the present moment, India continues to engage in a process of regulatory discussion. Ongoing dialogues and talks among governmental entities, industry participants, and subject matter experts persistently influence the prospective regulatory framework for cryptocurrencies and blockchain technology inside the nation.

The fluctuation between restriction and acceptance seen in India signifies the complex strategy used by authorities in addressing the disruptive capabilities of new technologies. The Indian government acknowledges the need to achieve a harmonious equilibrium between promoting innovation and mitigating possible hazards, including money laundering, and ensuring consumer protection.

The legal trajectory of India pertaining to cryptocurrencies and blockchain serves as a representative example of the worldwide predicament confronted by governments in accommodating this revolutionary technology. With ongoing talks and the

[40] Internet and Mobile Association of India vs. Reserve Bank of India 2020 INSC 264.

evolution of legal frameworks, the cryptocurrency ecosystem in India is anticipated to undergo significant growth, possibly exerting influence on the trajectory of these technologies inside the nation and globally.

VI. CHALLENGES AND SOLUTIONS IN CROSS-BORDER TAXATION

The absence of borders inherent in cryptocurrencies and the decentralised framework of blockchain technology has engendered a distinct array of obstacles within the domain of taxes. This part aims to discuss the aforementioned difficulties and examine novel approaches to ensure the efficacy of cross-border taxes in the context of the digital age.

A. Assessing and Collecting Taxes in a Borderless Environment

The decentralised character of cryptocurrencies, in conjunction with the widespread accessibility of blockchain networks, poses a notable obstacle in the precise evaluation and collection of taxes. In contrast to conventional financial systems, which heavily rely on middlemen to facilitate transactions, cryptocurrencies enable direct transfers between peers across international boundaries, eliminating the need for intermediaries. The underlying nature of these transactions poses significant challenges for tax authorities in their efforts to trace and regulate them[41].

One plausible approach is the use of blockchain analytics and tracking systems. These technologies use the inherent transparency of blockchain ledgers to track the movement of money and ascertain the identities of individuals or entities participating in crypto transactions. Through the application of sophisticated data analytics and artificial intelligence techniques, tax authorities can acquire valuable insights pertaining to the movement of cryptocurrencies, thereby facilitating the precise evaluation and determination of tax liabilities.

---

[41] *Crypto solutions for Tax Agencies* CHAINALYSIS. (Jan. 14, 2025). https://www.chainalysis.com/tax-agencies/

Moreover, the establishment of collaborative efforts between tax authorities and cryptocurrency exchanges might enhance the process of reporting transaction data. This collaboration has the potential to facilitate the creation of automated reporting systems, whereby exchanges provide comprehensive transaction records to tax authorities, hence facilitating more accurate tax computations.

B. Jurisdictional Authority and Concerns Regarding Information Sharing

The challenge of ascertaining jurisdictional authority within the realm of cross-border crypto transactions is a multifaceted one. Conventional tax regimes often adhere to geographical limitations, but cryptocurrencies function within a decentralised and global context. This situation prompts inquiries over the jurisdiction that has the legitimate entitlement to tax profits derived from global cryptocurrency transactions.[42]

In order to effectively tackle this situation, it is essential to prioritise international collaboration and establish agreements between nations. Bilateral or multilateral agreements have the capacity to develop unambiguous frameworks for the taxation of cross-border cryptocurrency transactions, so assuring the equitable allocation of income among the countries concerned.

Moreover, the exchange of information across nations is necessary for the efficient implementation of cross-border taxes. The implementation of safe and standardised protocols for the transmission of pertinent tax information within the bitcoin ecosystem may effectively address issues related to tax evasion and enhance transparency.

C. *Innovative Approaches to Preventing Tax Evasion and Ensuring Compliance*

[42] *International standards for Automatic Exchange of information in Tax Matters.* OECD. (Jan. 14, 2025) https://www.oecd.org/en/publications/2023/06/international-standards-for-automatic-exchange-of-information-in-tax-matters_ab3a23bc.html

The implementation of innovative strategies is crucial in the prevention of tax evasion and the promotion of compliance within the realm of cryptocurrencies. One such strategy is the use of smart contracts as a means of enforcing tax compliance. Smart contracts are contracts that are capable of self-execution, whereby the terms and conditions of the agreement are explicitly encoded into computer code. These systems have the capability to do automated tax calculations and deductions at the moment of transaction, guaranteeing prompt adherence to tax regulations.

Additionally, the use of token-based taxation models has the potential to significantly transform the process of tax assessment. This methodology entails the allocation of tax obligations to individual tokens, hence facilitating more precise tax computations. Moreover, the use of decentralised identification solutions may be employed to authenticate the identities of the entities engaged in crypto transactions, hence augmenting endeavours to ensure adherence to regulatory requirements.

The resolution of cross-border taxation complexities within the realm of cryptocurrencies and blockchain technology necessitates the implementation of a comprehensive and diverse strategy. By using blockchain data, fostering international collaboration, and embracing novel tax enforcement strategies, policymakers may devise efficacious approaches to traverse the intricacies of a financial world without borders. The implementation of these progressive strategies will play a crucial role in guaranteeing the continued relevance and adaptability of tax policy within the swiftly changing digital economy.

VII. CRAFTING NUANCES POLICIES AND ADAPTIVE TAXATION POLICIES

A. Urgency for Responsive Taxation Policies in Asia

The exponential growth of cryptocurrencies and blockchain technology has necessitated the development of proactive taxation rules in the Asian region. The sense of urgency originates from the disruptive nature of these developments, which pose challenges to established financial institutions and need a prompt reaction from

regulators. The delayed implementation of efficient taxation policies has the potential to result in significant financial losses for governmental entities. Moreover, this phenomenon might potentially provide difficulties in the realm of financial stability and the protection of investor interests.[43]

The dynamic characteristics of the bitcoin industry provide an additional level of intricacy. The dynamic landscape of technology, evolving consumer preferences, and the constant introduction of novel financial instruments need tax rules that are flexible and responsive. The use of static frameworks, which are not well-adapted to the dynamic characteristics of cryptocurrencies, may result in inefficiencies and impede the development potential of the industry.

Furthermore, the absence of well-defined taxation laws creates a sense of unpredictability for both firms and people engaged in activities linked to cryptocurrencies. The presence of uncertainty has the potential to discourage investment and hinder innovation within the industry, which might have adverse effects on economic growth and development. Hence, the need for proactive taxing policies in Asia is not just a question of fiscal prudence but also a strategic requirement for cultivating a favourable atmosphere for technological innovation.

B. *Balancing Technological Innovation with Effective Taxation*

The attainment of a nuanced equilibrium between technical advancement and efficient taxation is a key concern for policymakers in the Asian region. The domain of cryptocurrency and blockchain presents a promising pathway for substantial technical progress, with the ability to stimulate economic development, augment financial inclusivity, and transform the level of transparency in financial activities.

Concurrently, taxes continue to serve as a vital mechanism for financing governmental activities and facilitating the provision of public services. The primary

---

[43] *From tax havens to high-tax regions, an overview of cryptocurrency taxation in Asia*. CHAINCATCHER, (Jan. 14, 2025), https://www.chaincatcher.com/en/article/2158041

objective is to guarantee the equitable distribution of the advantages derived from technological advancements across society. Achieving this equilibrium necessitates the examination of novel tax frameworks that are in line with the distinctive attributes of cryptocurrencies. Furthermore, the incorporation of incentives for research and development in the field of blockchain technology inside tax regimes might serve as an additional driver for encouraging and stimulating innovation.[44]

The maintenance of this equilibrium is crucial for cultivating a milieu that is conducive to the flourishing of technical advancements, all the while guaranteeing an equitable distribution of the tax burden. A comprehensive strategy is necessary that recognises the potential advantages of these advancements and considers the financial obligations of governing bodies.

C. *Imperative of Cross-Border Cooperation for Responsible Growth*

The absence of borders in cryptocurrencies and the widespread availability of blockchain networks provide a distinct taxation difficulty. The seamless occurrence of transactions between jurisdictions presents a significant challenge for individual countries in properly enforcing tax compliance. Hence, it is crucial to establish a significant degree of collaboration across national borders.

The establishment of information-sharing agreements and fostering cooperation in taxation enforcement play crucial roles in promoting responsible development within the bitcoin industry. It is essential for nations to collaborate in order to develop shared standards and optimal methodologies for the taxation of activities associated with cryptocurrencies. This measure not only serves as a deterrent against tax cheating but also cultivates a climate of trust and collaboration among governments.

---

[44] Ekshian, E. *Japan leads in global crypto innovation with Green Mining & Tax Reforms*. CRYPTO COUNCIL FOR INNOVATION, (Jan. 14, 2025), https://cryptoforinnovation.org/japan-leads-in-global-crypto-innovation-with-green-mining-tax-reforms

In addition, international organisations and conferences serve as crucial facilitators of cross-border collaboration. The establishment of platforms dedicated to facilitating debate and knowledge-sharing on cryptocurrency taxes has the potential to foster the creation of unified and mutually beneficial methods that cater to the interests of all relevant parties. The need to foster cross-border collaboration is fundamental in guaranteeing the conscientious and enduring development of bitcoin and the blockchain ecosystem at a worldwide level.

VIII. IMPLICATIONS OF ACCEPTANCE OF CRYPTO-CURRENCIES FOR ASIAN ECONOMIES

The diverse and far-reaching ramifications of cryptocurrencies and blockchain technology for Asian economies are evident. The use of these technologies can profoundly transform economic environments, offering both prospects and obstacles that need prudent navigation.

The integration of cryptocurrencies with blockchain technology has the potential to stimulate economic development via the cultivation of an environment that encourages innovation and entrepreneurship.[45] Asian countries that strategically position themselves as early adopters in this domain have the potential to acquire a competitive advantage in the international market. By fostering the growth of Startups and research efforts, these economies have the potential to develop into centres of technological innovation, drawing in skilled individuals and investment from many global sources.

The ability to enhance financial inclusion is seen as one of the most promising attributes of cryptocurrencies. A considerable proportion of the population in several Asian nations continues to lack access to formal banking services or has limited access

[45] *Blockchain gaining ground in Southeast Asia*. ASEAN CENTRE FOR ENERGY, (Jan. 14, 2025) https://aseanenergy.org/news-clipping/blockchain-gaining-ground-in-southeast-asia/

to such services.[46] Blockchain technology has the potential to provide safe and easily accessible financial services, enabling people to actively participate in the formal economy, get credit, and engage in international commerce.

The inherent transparency and immutability of blockchain technology can bring about significant transformations in several sectors, such as supply chain management, healthcare, and government services. Asian economies have the potential to use this technology to establish systems that are more efficient and transparent[47], hence reducing corruption and safeguarding the reliability of crucial procedures.

The emergence and increasing prominence of cryptocurrencies provide a formidable obstacle to conventional financial systems and organisations. Central banks and regulatory bodies are faced with the imperative task of conscientiously deliberating on the optimal approach to incorporating or overseeing these emerging VDAs. Maintaining an optimal equilibrium between innovation and stability will be of utmost importance in mitigating possible shocks to existing financial institutions.

The cryptocurrency industry has seen significant expansion, accompanied by inherent hazards such as price volatility, cybersecurity vulnerabilities, and susceptibility to fraudulent operations. In order to ensure the security of people and companies involved in cryptocurrency transactions, it is imperative for Asian economies to adopt strong risk management mechanisms[48] and consumer protection legislation.

Asian countries that strategically position themselves as frontrunners in the realm of cryptocurrencies and blockchain technology have the potential to significantly bolster

---

[46] Kapron, Z. *Why emerging southeast asia is crypto friendly*, FORBES. (Jan. 14, 2025) https://www.forbes.com/sites/digital-assets/2023/05/14/why-emerging-southeast-asia-is-crypto-friendly

[47] Richter, F.-J. *Using blockchain more broadly across Asia*, HORASIS. (Jan. 14, 2025). https://horasis.org/using-blockchain-more-broadly-across-asia

[48] *India leads in crypto adoption for second straight year.* REUTERS. (Jan. 14, 2025). https://www.reuters.com/technology/india-leads-crypto-adoption-second-straight-year-report-shows-2024-09-11

their global competitiveness.[49] These technological advancements enable smooth cross-border transactions, perhaps leading to a decrease in transaction expenses and an enhancement in the effectiveness of global commerce.

The use of cryptocurrencies and blockchain technology also poses regulatory issues. Asian countries must strategically design and modify regulations to guarantee the responsible use of new technologies while adhering to established legal frameworks. Achieving an optimal regulatory equilibrium is of paramount importance in promoting innovation while also mitigating possible hazards.

The enormous ramifications of cryptocurrencies and blockchain technology for Asian economies are evident. Although there exist considerable prospects for economic expansion, financial inclusivity, and technical supremacy, there also exist noteworthy obstacles that need adept navigation. Through a meticulous examination of these ramifications and the implementation of discerning strategies, Asian countries have the potential to establish themselves as frontrunners in the worldwide digital economy.

IX. CONCLUSION

From Japan's legalisation of Bitcoin to China's strict regulation and Singapore's clarification, Asian governments have taken different approaches. As examined, these techniques affect investor sentiment, technical innovation, and the crypto ecosystem in each country.

Blockchain technology's decentralisation, cross-border transactions, and anonymity make tax assessment and collection difficult. Cryptocurrencies are borderless, raising jurisdictional issues and requiring extensive cross-border collaboration.

---

[49] *Southeast Asia emerges as Crypto, blockchain, and Ai Hub*. COMMERCIAL POLICY INTERNATIONAL. (Jan. 14, 2025). https://www.pymnts.com/cpi-posts/southeast-asia-emerges-as-crypto-blockchain-and-ai-hub

South Korea's real-name trading accounts and Singapore's comprehensive Payment Services Act demonstrate openness, accountability, and regulatory compliance. These initiatives demonstrate the need for dynamic adaptability in this changing digital context.

Due to cryptocurrencies' disruptive nature and fast technical advancement, appropriate taxation rules are needed. Failure to establish appropriate taxation policies might cost governments income and financial stability. The lack of clear taxation rules may also limit industry innovation and investment.

Effective taxes and technological innovation must be balanced. For global competitiveness, bitcoin and blockchain innovation must be encouraged. Taxation is necessary to support government and public services. To achieve this balance, cryptocurrency-specific tax structures must be explored.

Taxing cryptocurrencies and blockchain networks is difficult due to their worldwide reach. Transactions may easily transcend countries, making tax compliance difficult for any one nation. Countries must cooperate extensively across borders. The growth and stability of Asian economies depend on creating complex and flexible taxation laws to address cryptocurrencies and blockchain technologies. In this transformational digital world, cross-border collaboration is needed to avoid tax evasion and promote responsible development via technical innovation and efficient taxation.

For long-term economic development and stability, Asian nations must balance innovation and taxes as they embrace the digital revolution. The future demands smart policy, innovative regulations, and international cooperation. Asian economies can influence digital finance by foreseeing and being careful.

Asian countries have a revolutionary potential as cryptocurrencies and blockchain technologies have revolutionised financial innovation. However, this climb is

difficult. Policymakers and regulators must create responsive taxation rules in the face of fast technological change.

CHARTING A BALANCED COURSE: SAFEGUARDING CONSUMER RIGHTS IN THE AGE OF AI INNOVATION

- HIMANSHU CHIMANIYA & VISHRUT VEERENDRA

ABSTRACT

*In the age of Artificial Intelligence ("**AI**"), consumer rights are increasingly at risk. AI relies on data and algorithms, often manipulating consumer behaviour through coercive tactics. Consumers' data is extracted via non-negotiable, broadly worded contracts, undermining their autonomy. Additionally, AI-enabled products present new challenges, as existing laws fail to mandate transparency about their functioning, limiting consumers' right to be informed. Current product liability laws inadequately address defects, unfairly shifting responsibility between manufacturers and consumers, disrupting market fairness.*

This paper examines AI-driven data collection by digital enterprises, analysing weak consumer and data protection laws that fail to regulate observed data and contracts, leading to rights violations. It also assesses Indian and European product liability laws, which insufficiently address harms from defective AI-enabled products. The paper advocates for limiting observed data collection, enhancing consumer awareness of AI's data-processing mechanisms, and ensuring informed consumer choices. It calls for stronger regulatory intervention in data contracts, an ex-ante approach to AI-enabled products, and reforms in product liability to sustain a fair and trusted market.

The paper proposes key reforms to safeguard consumer rights while ensuring the responsible and beneficial use of AI technology.

Keywords – Artificial Intelligence, Consumer Rights, AI-enabled Products, Data Collection Contracts, Defects, Product Liability, Ex-ante Approach

I. INTRODUCTION

As witnessed in past decades, the use of artificial intelligence has grown significantly; and considering the pace with which its use is growing, one cannot foresee a future without artificial intelligence. Since 1994, when the first e-commerce transaction was done in India[1], the landscape of Indian markets has completely changed. Today, a huge part of the Indian population is using the digital market. It is growing at a rate of 25% to 30% rate per year and its value is expected to grow to 539 (five hundred thirty-nine) billion rupees by the end of 2024.[2] The inclusion of AI has exemplified the growth of this sector.[3] Rapid technological improvement, in AI and Machine Learning has transformed digital marketing. The progression of AI in the present day is revolutionizing customer communication and marketing strategies. Digital enterprises are using AI in full swing to maximize their sales and profit.

The functioning of AI is different from previous technological advancements.[4] The functioning of AI involves the use of advanced algorithms to create systems capable of performing tasks autonomously, often through self-generated recommendations and decision-making.[5] As explained by NITI Aayog, "AI comprises algorithms that enable machines to emulate human intelligence by sensing, comprehending, and acting." AI perceives its surroundings using technologies like computer vision and audio processing, which allow it to process images, sound, and speech. It analyses and

---

[1] Neeta Aurangabadkar Pole, *Digital Marketing in India – Its Evolution and Growth*, 8 NAT. VOLATILES & ESSENT. OILS 308-320 (2021).

[2] Preneshraj N.M., R. Arunprakash, *Expansion And Penetration Of Digital Marketing In India*, 8 INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY 57-64 (2024).

[3] Adib Bin Rashid, MD Ashfakul Karim Kausik, *AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications*, 7 HYBRID ADVANCES (2024).

[4] Robbie Allen, *Why Artificial Intelligence is Different from Previous Technology Waves*, MEDIUM (June 13, 2017)https://robbieallen.medium.com/why-artificial-intelligence-is-different-from-previous-technology-waves-764d7710df8b. (last accessed on 11th February, 2025)

[5]Council of Bars and Law Societies of Europe, *Considerations on the Legal Aspects of Artificial Intelligence*, CCBE COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE (2020), https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20200220_CCBE-considerations-on-the-Legal-Aspects-of-AI.pdf. (last accessed on 11th February, 2025)

understands information through natural language processing and inference engines. Additionally, AI can act using expert systems and interact with the physical world. Its ability to learn and adapt over time further enhances these processes, enabling AI to become increasingly sophisticated and widely applied across industries to expand and enhance their capabilities.[6]

AI systems utilise data sets to generate results, analysing user behaviour to improve and provide personalised experiences.[7] In the digital market, AI enhances interactions through tailored recommendations, optimised searches using voice commands or images, and augmented reality shopping, allowing customers to visualise items like furniture or clothing in their space before purchase.[8] AI-enabled products such as self-driving cars improve safety by reducing human error, while smart home assistants enhance energy efficiency by adapting to user habits.

While AI drives innovation and benefits both consumers and enterprises, unchecked deployment risks creating disproportionate advantages for digital enterprises and endangering consumer welfare.[9] This paper examines these challenges: the first section explores how digital enterprises use AI for data collection and processing, and the second addresses defects in AI products, such as design flaws and biased algorithms, and their impact on consumer rights.

---

[6] NITI AAYOG, NATIONAL STRATEGY FOR ARTIFICIAL INTELLIGENCE 2017-18 12 (2018).

[7] Abid Haleem, *Artificial intelligence (AI) applications for marketing: A literature-based study*,3 INTERNATIONAL JOURNAL OF INTELLIGENT NETWORKS 119-132 (2022).

[8] Yogita Yashveer Raghav, *The Future of Digital Marketing: Leveraging Artificial Intelligence for Competitive Strategies and Tactics*, RESEARCHGATE (November 2023) https://www.researchgate.net/publication/375731424_The_Future_of_Digital_Marketing_Leveraging_Artificial_Intelligence_for_Competitive_Strategies_and_Tactics. (last accessed on 11th February, 2025)

[9] George Benneh Mensah, *Artificial Intelligence and Ethics: A Comprehensive Review of Bias Mitigation, Transparency, and Accountability in AI Systems*, RESEARCHGATE (2023) https://doi.org/10.13140/RG.2.2.23381.19685/1. (last accessed on 11th February, 2025)

II. AI-ENABLED SERVICES: ADEQUACY OF INDIAN LAWS

A. Definition of Data under the Digital Personal Data Protection Act,2023

Data is defined under the recently implemented Digital Personal Data Protection Act, 2023 **("DPDP Act").** As per the definition provided in it, "Data means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means".[10] It regulates personal data used by digital platforms and also includes interpretations of such data. As per the DPDP Act, digital enterprises shall request from the consumer the data they want, mentioning the purpose of collecting and processing it.[11] DPDP Act prohibits unlawful use of data and where consumers have explicitly denied[12] the processing of their data[13]. Yet a huge domain of data is not protected. Only personal data, which means any data about an individual who is identifiable by or in relation to such data,[14] and the interpretations made out of it are regulated.

B. Misuse of Data Using AI

Apart from personal data of individuals that is observed by digital enterprises[15] like online search one makes on search engines, and interpretation made from that huge data set can be used for any purpose which is not strictly prohibited by law. There is no settled mechanism for the processing of data.

However, along with the benefits, AI influences consumers' decision-making process by using its data in many ways such as product recommender systems, personalized

---

[10]Digital Personal Data Protection Act, 2023, § 2(h), No. 22, Acts of Parliament, 2023 (India).
[11] *Id*, § 5.
[12] *Id*, § 7.
[13] *Id*, § 4(ii).
[14]*Id*, § 2(t).
[15]JUSTICE B.N. SRIKRISHNA COMMITTEE, WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA 142 (2018).

shopping experiences, and digital market manipulation.[16] AI systems can manipulate consumers to buy products from a certain seller by showing their product on top of search results, targeted advertisements, or by other means affecting consumers' right to choose.[17] There is a long list of practices that are deployed by digital enterprises to affect consumer behaviour resulting in the breach of consumer rights. Central Consumer Protection Authority **("CCPA")** has released the Guidelines for Prevention and Regulation of Dark Patterns, 2023[18], in pursuance of such practices.[19]

Among numerous malpractices, thirteen flagged by the CCPA are now prohibited as per the said guidelines.[20] These practices include false urgency, which means falsely implying a sense of urgency or a high demand to mislead consumers into making an immediate purchase or action, which ultimately benefits the digital enterprise.[21] AI can analyse consumers' behavioural data to predict the needs and the proper time to create a sense of urgency to increase the price of certain goods or services. For example, it can falsely present data on high demand without appropriate context "Only 2 rooms left! 30 others are looking at this right now." Next in line is basket sneaking, in which AI can automatically include additional items at checkout by analysing data related to consumers' previous purchases and behaviours.[22] For example, it can automatically add travel insurance when a user purchases a flight ticket. Bait and switch by which AI can change the availability or pricing of products

---

[16] Shuo Wang, *The Influence of AI in Marketing*, ADVANCES IN ECONOMICS MANAGEMENT AND POLITICAL SCIENCES 151(1):52-57 (JANUARY 2025) https://www.researchgate.net/publication/387777644_The_Influence_of_AI_in_Marketing. (last accessed on 11th February, 2025)

[17] Consumer Protection Act, 2019, § 2(9)(ii), No. 35, Acts of Parliament, 2019 (India).

[18] Guidelines for Prevention and Regulation of Dark Patterns, Gazette of India, pt. III sec.4, (Nov. 30, 2023).

[19] ET Online, *Beware of Drip Pricing, says govt. What is drip pricing? How to stay safe?*, THE ECONOMIC TIMES, (May 08, 2024) https://economictimes.indiatimes.com/news/company/corporate-trends/beware-of-drip-pricing-says-govt-what-is-drip-pricing-how-to-stay-safe/govt-sounds-warning/slideshow/109947353.cms. (last accessed on 11th February, 2025)

[20] Guidelines for Prevention and Regulation of Dark Patterns, Gazette of India, pt. III sec.4, (Nov. 30, 2023), Rule 4.

[21] *Id*, Entry i, Annexure 1.

[22] *Id*, Entry ii, Annexure 1.

based on previous actions of a consumer, to lure them into purchasing more expensive items.[23] AI can create advertisements that blend with other content to confuse consumers into clicking on them to earn through clicks.

Digital technology is deeply embedded in our lives. Everything is recorded, whether on social media, e-commerce sites, or at local retailers. At every step along this process, data is being generated.[24] From the above examples of malpractices by digital platforms, it is evident that this data can be exploited. Shopping behaviour data alone can reveal personal information about a consumer.[25] For instance, if a consumer books flight tickets and buys luggage, AI can predict that the person has travel plans. And, subsequently, AI can use this information to manipulate consumer's actions using the above-mentioned practices.[26] AI has the ability to stimulate spending, direct product choices, or target promotions challenges the right to make consequent personal decisions. Consumer law safeguards the private autonomy of consumers and protects their economic rights.[27] Certain loopholes in current consumer protection laws could be misused by AI.

C. Loopholes in Present Laws

The present Consumer Protection Act, 2019 (**"CPA"**) takes into consideration the prevalent digital market.[28] However, it does not dive into the aspect of the use of AI by digital enterprises. We have established that AI models can exert undue influence on consumers and push them to make decisions they would not have otherwise taken.

---

[23] *Id*, Entry vii, Annexure 1.

[24] ETHEM ALPAYDIN, INTRODUCTION TO MACHINE LEARNING, 1-20 (3rd ed. 2014).

[25] Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in Privacy and Self-Regulation in the Information Age by the U.S. Department of Commerce.*, GEORGIA INSTITUTE OF TECHNOLOGY (10 Jun 2017) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=11472. (last accessed on 11th February, 2025)

[26] *Supra* note 21.

[27] Consumer Protection Act, 2019, § 2(9)(iii), No. 35, Acts of Parliament, 2019 (India).

[28] *Id,* § 2(16).

To effectively implement the rights granted to consumers in the age of AI, a few additional measures have to be taken.

i. Information Gap

Access to extensive consumer data enables digital enterprises to understand their customers better, often infringing on consumer rights. While AI offers benefits like personalised recommendations, consumers remain largely unaware of how their data is processed and the quality of the advice given. The lack of transparency about data handling and AI decision-making leaves consumers unable to discern how their data influences outcomes. Although the DPDP Act requires specifying a purpose for data collection and processing[29], the methods to achieve this aim are still unclear. The current DPDP Act framework's notice and consent provisions do not sufficiently address the misuse of personal data or regulate observed data processing, which significantly impacts consumer rights.[30] Moreover, while the CPA provides consumers with the right to be informed and make free choices[31]. AI often limits this autonomy without full transparency. Consumers are informed only about the purpose of data collection, while the underlying processes remain hidden. This lack of clarity undermines the assumption that consumers are fully informed and making genuinely free choices.

ii. Bogus Agreements

Data processing agreements are often drafted in broad, unilateral, and non-negotiable terms by data controllers, which once accepted by consumers, affects their data protection rights due to a lack of transparency.[32] The DPDP Act requires that consent

[29] Digital Personal Data Protection Act, 2023, § 5(1)(i), No. 22, Acts of Parliament, 2023 (India).
[30] *Id*, § 4,5.
[31] Consumer Protection Act, 2019, § 2(9), No. 35, Acts of Parliament, 2019 (India).
[32] Christof Koolen, *Transparency and Consent in Data-Driven Smart Environments*, 7 EUROPEAN DATA PROTECTION LAW REVIEW 186 (2021).

from data principles be free, specific, informed, unconditional, and unambiguous.[33] However, consumer consent for observed data might not always meet these standards. While the CPA addresses unfair contracts, it does not specifically cover data collection and misuse. Under the Act, "unfair contract" refers to agreements between a manufacturer, trader, or service provider and a consumer that significantly alter the consumer's rights.[34] The broadest interpretation of unfair contracts could encompass manipulative practices through AI. Nevertheless, distinguishing between legitimate personalised advertising and undue influence can be challenging. The AI era demands a more stringent and robust mechanism to safeguard consumer rights.

III. AI-ENABLED PRODUCTS: ADEQUACY OF INDIAN LAWS

A. Defects in AI-enabled products

As the adaptation of AI is growing in society, a greater possibility of various violations of law is evident. There is a need to restructure the present legal system to deal with the dynamic and complex nature of the situation. The globe is witnessing various incidents that resulted in gross injury just because consumers relied on AI. In 2016, there was a serious incident where a self-driving vehicle did not recognize a tractor-trailer due to the bright sky.[35] Another is a medical AI system that is used to detect diseases but the same has many times generated false positives.[36] Robodebt was an automated system designed for the Australian Government to collect debts by comparing individuals' financial data to identify discrepancies. However, it mistakenly issued debt notices to hundreds of thousands of people, leaving them to

---

[33] Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).
[34] Consumer Protection Act, 2019, § 2(46), No. 35, Acts of Parliament, 2019 (India).
[35] Yadron & Tynan, *Tesla driver dies in first fatal crash while using autopilot mode*, THE GUARDIAN (July 1, 2016) https://www.theguardian.com/technology/2016/jun/30/tesla-autopilot-death-self-driving-car-elon-musk. (last accessed on 11th February, 2025)
[36]Taro Makino, Stanisław Jastrzębski, Witold Oleszkiewicz, *Differences between human and machine perception in medical diagnosis*. SCIENTIFIC REPORTS (April 27, 2022) https://www.nature.com/articles/s41598-022-10526-z. (last accessed on 11th February, 2025)

challenge the erroneous calculations made by the system.[37] These are only few examples of how AI enabled products can result in injury. As more and more products adopt AI, more cases of blunder will emerge. The main complexity that exists in this scenario is related to autonomous AI systems, where technology works without direct involvement of producer. In such cases neither the user nor the producer has full control over the device and if such a device results in injury, the liability becomes the central question.

B. Control over AI-enabled products

AI-enabled products possess the remarkable ability to make decisions independent of the provided dataset and without human intervention by utilizing advanced techniques such as machine learning,[38] deep learning,[39] and neural networks.[40] These systems are designed to identify patterns, learn from prior interactions, and adapt to new scenarios. Through reinforcement learning, they optimize decision-making based on outcomes and feedback. Pre-trained models and algorithms further enhance their capabilities by enabling them to generalize knowledge, predict outcomes, and respond dynamically to novel inputs, without relying solely on a static dataset or manual oversight. For instance, a security camera that records only upon detecting motion showcases how AI systems act independently and intelligently in real-time.

---

[37] LH Gomes, *Robodebt: Government to Refund 470,000 Unlawful Centrelink Debts Worth $721 M*, THE GUARDIAN (May 29, 2020) https://www.theguardian.com/austraha-news/2020/may/29/robodebt-govemment-to- repay-470000-unlawful-centrerink-debts-worth-721m. (last accessed on 11th February, 2025)

[38]Emma Crockett, *What is Machine Learning*, DATAMATION (July 17, 2023) https://www.datamation.com/big-data/what-is-machine-learning/. (last accessed on 11th February, 2025)

[39] Doug Black, *AI Definitions: Machine Learning vs. Deep Learning vs. Cognitive Computing vs. Robotics vs. Strong AI,* AI WIRE (May 30, 2019) https://aiwire.net/2019/05/30/ai-definitions-machine-learning-vs-deep-learning-vs-cognitive-computing-vs-robotics-vs-strong-ai-2/. (last accessed on 11th February, 2025)

[40] Stephen DeAngelis, *Artificial Intelligence Terms,* ENTERRA SOLUTIONS (July 20, 2020) https://enterrasolutions.com/artificial-intelligence-terms/. (last accessed on 11th February, 2025)

However, such autonomy also raises significant concerns. Semi-automatic AI-enabled products challenge traditional notions of responsibility, as neither manufacturers nor users have full control over these systems. This lack of control can lead to complex liability issues, particularly when malfunctions occur. Accidents involving self-driving cars highlight this challenge, as flaws in the product design[41] often cause harm. Users expect these systems to operate independently, while manufacturers might not fully oversee AI systems with autonomous capabilities. Autonomy, by its nature, allows AI to make decisions based on rules that are not entirely pre-defined, leading to unforeseen outcomes. In such cases, determining liability and whether such decisions constitute defects[42] under the Consumer Protection Act remains an ongoing legal and ethical debate.

i. Liability of AI

The primary question is whether AI can be held liable for its actions. Currently, AI does not have legal personality in international and national laws but this could change in the future. Under the CPA the inclusive definition of the term 'person' includes an artificial juridical person[43] which broadens the scope for imputing liability. Including AI as a 'person' would require extensive debate because liability for injury caused by a product or service is currently attached to real human beings, such as manufacturers or sellers, not to artificial systems. Additionally, CPA does not envision imposing liability on a networking system or any other technological advancement in product manufacturing, but rather on the creator of the product itself. [44]

---

[41] Sunghyo Kim, *Crashed software: Assessing product liability for software defects in automated vehicles*, 16 DUKE LAW & TECHNOLOGY REVIEW, 300–317 (2018).
[42] Consumer Protection Act, 2019, § 2(10), No. 35, Acts of Parliament, 2019 (India).
[43] *Id*, § 2 (31)(vii).
[44] *Id*, § 2(36).

ii. Concept of Defect

The CPA defines a defect as any fault, imperfection, or shortcoming in the quality, quantity, potency, purity, or standard required to be maintained by or claimed by the trader[45]. This definition does not clearly encompass unforeseeable injuries caused by AI-enabled products, as their quality and standards might not be faulty.

For instance, an autonomous vacuum cleaner designed to navigate and clean floors might collide with and cause damage due to a software glitch. Despite the robot's intact quality and standards, its decision-making process caused unintended harm. Manufacturers might argue such harm was unforeseeable, given the AI's self-learning capabilities based on consumer interaction, leaving consumers in a helpless situation. The debate persists on whether the harm caused by AI-enabled products is due to a defect in the product or a design flaw.[46] Since these products operate on pre-determined data and instructions, their learning and improvement are rooted in this initial programming.

iii. Product Design

The defects in AI-enabled products often arise from issues in the design of the product rather than manufacturing flaws. These products operate using complex algorithms[47] and their functionality depends on various design factors such as training data, learning algorithms, model architecture, and decision-making rules.[48] Since AI systems primarily rely on software components, flaws in the software code can

---

[45] *Id*, § 2(10).

[46] *What are the advantages & disadvantages of Robot Vacuums*, ECOVACS (November 22, 2024) https://www.ecovacs.com/us/blog/advantages-and-disadvantages-of-robot-mop-vacuum. (last accessed on 11th February, 2025)

[47] *Supra* note 4.

[48] Catherine Sharkey, *Products Liability for Artificial Intelligence*, LAWFARE (September 25, 2024) https://www.lawfaremedia.org/article/products-liability-for-artificial-intelligence. (last accessed on 12th February, 2025)

significantly impact their performance, leading to defects.[49] Such design defects may include biases in the training data, errors in the algorithms, or insufficient consideration of rare or unexpected scenarios. Unlike traditional products where errors may stem from the assembly line, defects in AI systems are typically rooted in how they are conceived and developed. Therefore, when problems occur, they are more likely the result of design issues rather than manufacturing defects.

The CPA deals with design defects. However, it delves only into the product's design, and physical and material characteristics of the product, not its internal components.[50] It does not focus on AI-enabled products whose design consists mainly of internal components such as data, set of instructions, and algorithms. Thus, it focuses only on the product's appearance and functionality rather than its internal mechanisms. This inadequacy left consumers unprotected from the harms that occur from defective designs of AI-enabled products.

In cases where a consumer faces harm because of an AI-enabled product resulting from a design defect, it is difficult to prove such a defect.[51] While identifying manufacturing defects is usually straightforward, proving design defects is more challenging especially when it pertains to research and development and product design issues.[52] An average consumer is not expected to have adequate knowledge of how an AI system should be designed, and the burden of proof that the harm is a result of a design defect is difficult to establish.

---

[49] M.C. Buiten, *Product liability for defective AI*. EUR J LAW ECON 57, 239–273 (2024) https://doi.org/10.1007/s10657-024-09794-z. (last accessed on 12th February, 2025)

[50] Consumer Protection Act, 2019, § 2(12), No. 35, Acts of Parliament, 2019 (India).

[51] Megan Howarth, *AI liability – who is accountable when artificial intelligence malfunctions?*, TAYLORWESSING (January 7, 2025) https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/ai-liability-who-is-accountable-when-artificial-intelligence-malfunctions. (last accessed on 12th February, 2025)

[52] Chadwick D. Meyers, *The Differences Between Manufacturing Defects and Design Defects in Tennessee: A Clear Distinction*, MEYERS INJURY LAW (January 24, 2024) https://meyersinjurylaw.com/blog/the-differences-between-manufacturing-defects-and-design-defects/. (last accessed on 12th February, 2025)

C. Consumer Awareness

Considering that neither the user nor the manufacturer has complete control over AI-enabled products, the prevention of harm is difficult. Products are designed to perform tasks, but it is not always clear how many complexities they can deal with within. Consider the example of an autonomous self-driving car, although it can drive by itself, but the question arises of how it would deal with certain nuanced situations. AI systems operate in a designated manner but beyond their programming they need human intervention. A lawsuit filed against Tesla illustrates the principle where plaintiffs argued that the automated driving technology had a flawed design because it did not provide alerts to a distracted driver.[53] AI systems are not always designed to alert human when there is a possibility of error in their functioning, they carry the motive of learning while dealing with new complexities. The distinction and division of responsibility between AI and humans is blurry concerning the use of such products. In a nutshell, consumers are not completely aware of the capabilities of AI-enabled products.

IV. FINDINGS

A. Insufficiency of Indian laws over AI enabled services

The extensive access to consumer data by digital enterprises has raised concerns about the infringement of consumer rights, especially with the advent of AI technologies. While AI offers advantages such as personalized recommendations, it lacks transparency in how consumer data is processed and how decisions are made. This obscurity leaves consumers largely unaware of how their data influences outcomes. Although the DPDP Act mandates that organizations specify the purpose of data collection and processing, the methods for ensuring compliance remain ambiguous.

---

[53] Sean Suber, Matthew Saxon, *First Lawsuit Filed for Tesla Autopilot-Related Death Involving a Pedestrian*, WINSTON & STRAWN LLP (June 16, 2020) https://www.winston.com/en/blogs-and-podcasts/product-liability-and-mass-torts-digest/first-lawsuit-filed-for-tesla-autopilot-related-death-involving-a-pedestrian. (last accessed on 13th February, 2025)

The Act's current framework, particularly its notice and consent provisions, does not adequately address the regulation of observed data processing, posing a significant threat to consumer rights. Additionally, while the CPA grants consumers the right to be informed and to make autonomous choices, AI systems often curtail this freedom by offering limited transparency regarding the actual data processing methods. As a result, consumers are led to believe that they are fully informed, when in reality, critical processes remain concealed, undermining their ability to make truly informed and free choices.

Secondly, data processing agreements, often drafted by data controllers, are typically broad, unilateral, and non-negotiable, reducing consumer data protection due to a lack of transparency. While the DPDP Act requires consent to be free, specific, informed, unconditional, and unambiguous, it does not account for how observed data may influence consumer behaviour, undermining genuine consent. The CPA addresses unfair contracts but does not cover the misuse of personal data. While the broad scope of "unfair contracts" could include exploitative AI practices, distinguishing between ethical advertising and manipulation is challenging. As AI increasingly shapes consumer interactions, concerns about transparency, accountability, and informed consent grow, highlighting the need for stronger legal frameworks to protect consumer rights, ensure equitable access, mitigate biases, and establish ethical guidelines for AI use.

B. Insufficiency in Indian laws over AI enabled products

The growing reliance on Artificial Intelligence across sectors has increased the likelihood of legal challenges, highlighting the need for a major update to existing legal frameworks. As AI adoption increases, more instances of harm and error are likely to emerge, raising critical questions about responsibility and accountability in such scenarios.

Moreover, AI-enabled products, capable of making independent decisions raise complex questions about liability and consumer protection. These systems often operate autonomously, reducing users' ability to prevent harm, as seen in self-driving car accidents caused by design flaws. The CPA lacks clarity on categorizing AI-related issues, particularly in distinguishing between product defects and design flaws. Proving these design defects is more challenging than identifying manufacturing defects, as average consumers lack the technical knowledge to recognize them. Additionally, AI systems do not always alert users when malfunctions occur, further complicating the division of responsibility between the AI and the human operator. As a result, consumers are often unaware of the limitations and risks associated with AI-enabled products, leading to potential harm from over-reliance on these systems.

V. SUGGESTIONS

A. Do away with Information Gap

To balance the rights of consumers and digital enterprises, it is essential to address the information gap between them. Legislation should mandate that enterprises disclose the actions taken by AI and the processes used to arrive at particular recommendations or insights. This transparency will enable consumers to exercise their right to be fully informed. Indian e-commerce regulations require marketplaces to inform consumers about the key parameters affecting product or seller rankings and their relative importance[54], yet this requirement is not sufficiently broad to address the wider scope of AI-related malpractices. It primarily targets self-preferencing in product rankings rather than the extensive range of issues AI can present. Consumers should be provided with clear information about the parameters and data used for personalised pricing, product ranking, search results, targeted advertising, and content personalisation. AI technology is constantly evolving and

[54] Consumer Protection (E-Commerce) Rules,2020, Gazette of India, pt. II sec.3(i), Rule 5(3)(f) (July 23, 2020).

inventing new methods to enhance business efficiency and profitability. As such, safeguarding consumer rights must remain a priority. By enabling consumers to have proper information about each action of AI and the process used behind it, they will be able to make free choices and will no longer be misguided using their own data. This approach not only benefits consumers but also contributes to a fair and trustworthy market environment.

B. Regulatory Intervention for Data Collection Contracts

The current data collection contracts significantly empower digital enterprises. In India, regulations only cover the collection and processing of personal data, leaving consumers with minimal control over how their data is processed once shared. AI can leverage data in numerous ways, creating an imbalance between the rights of consumers and the power of enterprises. Government intervention is necessary to address this imbalance. Existing contracts are based on consent rather than legal regulation, leading to a lack of accountability and transparency. To protect consumer rights, the government must implement regulations that address the collection and processing of data more comprehensively. These regulations should ensure that collection of observed data is subjected to same conditions as that of personal data. Additionally, they should enforce data minimisation principles and mandate clear information on data processing practices. While the protection of personal data is crucial, the regulation of observed data is also necessary for a complete consumer protection framework. This will ensure that AI's use of data does not undermine consumer rights and promotes a fairer market environment.

To effectively regulate this aspect of consumer protection, it is important to understand the distinction between automated systems and autonomous systems. An automated system functions independently while following pre-programmed instructions. For example, self-checkout kiosks in supermarkets allow customers to scan and pay for items independently, and robotic arms and conveyor belts in

manufacturing plants are used to assemble products. Conversely, an autonomous system possesses its own decision-making capacity.[55] For example, autonomous vehicles use sensors, cameras, and AI algorithms to navigate roads without human drivers. Autonomous drones for package delivery, that fly independently, avoiding obstacles and reaching specified destinations. On the question that who should be held liable for harms done by AI-enabled products, regulation is required. The manufacturer cannot always have control over the acts of AI-enabled products.

C. Ex-ante approach for autonomous products

Unforeseeable harms could be done by autonomous AI products. In such a situation, there must be an *ex-ante* approach to mitigate the risk posed by such products to protect the consumers. At present, there is no law dealing with AI explicitly.[56] A practical approach might involve utilizing regulatory and certification standards to define and address defects within AI systems. While designing AI systems, there must be guidelines on how they should be designed such as specifications for these systems and requirement for self-monitoring and fault-detection capabilities.[57] There should be a certification procedure that must be followed before introducing a product to the market. When designing AI systems, incorporating guidelines and specifications is crucial to ensure their reliability, safety, and effectiveness. In order to facilitate the same line of reasoning it will be beneficial if we adopt the European Union **("EU")** model which puts in line specific measures which should be taken care of before rolling any product or design in the market.

---

[55] Marilia A. Ramos and Ali Mosleh, *Human role in failure of autonomous systems: A human reliability perspective.* ANNUAL RELIABILITY AND MAINTAINABILITY SYMPOSIUM 1–6 (2021).

[56] Harsh Kumar and Vishal Singh, *Regulating AI: Navigating India's challenging regime*, ASIA BUSINESS LAW JOURNAL (April 15, 2024) https://law.asia/navigating-ai-india/#:~:text=The%20Digital%20India%20Act%20(DIA,governance%20frameworks%20are%20also%20essntial. (last accessed on 11 February 2025)

[57] Kumar, Nand & Groenewald, Elma & Kulkarni, Shailesh & Km, Ashifa. *Self-Healing Networks AI-Based Approaches for Fault Detection and Recovery*. 47 POWER SYSTEM TECHNOLOGY 371-386 (2023).

To ensure responsible AI development and deployment, regulations should be put in place to address AI-specific risks, EU has released its Artificial Intelligence Act ("**EU AI Act**"). From it, we can understand the aspect that has to be regulated to mitigate the possibility of harm arising from AI-enabled products. EU AI Act aims to prohibit practices that pose unacceptable risks, identifies high-risk applications, sets clear requirements for AI systems in those contexts, defines specific obligations for deployers and providers, mandates conformity assessments before market entry, enforces compliance post-market, and establishes national governance structures. [58]

European law categorises AI regulation into four parts: unacceptable risk, high risk, limited risk, and minimal risk. AI systems with unacceptable risks are banned outright, as they pose clear threats to safety, livelihoods, and rights. High-risk AI systems[59], which can significantly impact our lives, safety, and fundamental rights, and undergo rigorous assessment before and after market entry. High-risk products include critical infrastructure like transportation networks, and educational systems, safety-critical products such as AI-assisted surgery, and employment management tools like CV-sorting algorithms used in recruitment. Products posing significant risks and potential harm to consumers fall under this high-risk category.

Before these high-risk AI systems enter the market, they need to pass some tests of identifying, mitigation of risk, and continuous review throughout the product's lifecycle. This includes identifying and evaluating risks to health, safety, and rights, assessing risks from post-market data, and implementing mitigation measures. It also requires real-world testing, especially for impacts on vulnerable groups like minors.[60] Data inserted in these systems must be unbiased and high-quality.[61] These systems must record everything, what they do, its basis and how they do it, to ensure

---

[58]Artificial Intelligence Act, 2024, art. 57, Reg. (EU) 2024/1689 of European Parliament and of the Council, 2024 (European Union).
[59] *Id,* art. 9.
[60] *id*.
[61] *Id,* art. 10.

traceability of results.[62] Developers must specify the purpose of the AI system and its interoperability to ensure its compliance. There must be clear instructions to use such a system for users.[63] Developers must specify the extent of the need for human intervention. Such systems must be robust, secure and accurate.[64] The use of AI is essential to ease the tasks, but it has to be strongly checked to perform flawlessly, impactfully, and without any errors.[65]

However, it has to be noted that it only tackles the risks that could be reasonably mitigated or eliminated through the development or design of the high-risk AI system or the provision of adequate technical information and not the risks that are unforeseeable.

Including such provisions in Indian laws before launching any AI-enabled product in the Indian market will significantly reduce the possibility of harm through the use of AI. The absence of regulation in this aspect will lead to a situation where consumers will be hesitant to use new technology, and an untrustworthy market situation will arise. Therefore, an *ex-ante* approach is required to deal with autonomous AI products.

D. Consumer Awareness

For greater reliability and safety of autonomous systems an effective and informed human – machine interaction is must. This issue of ineffective human–machine interaction extends to all automated devices and not just AI. In 2019, Boeing 737 Max crashes illustrate this risk, where software failures resulted in pilot errors due to inadequate training and oversight.[66] An effective human–machine interaction is crucial for the autonomous systems.[67] Blind belief in AI can result in misuse, if users

---

[62] *Id,* art. 12.
[63] *Id,* art. 13.
[64] *Id,* art. 14.
[65] *Id,* art. 17.
[66] Chris Palmer, *The Boeing 737 Max Saga: Automating Failure*, 6 ENGINEERING 2-3 (2020).
[67] Marilia A. Ramos, Christoph A. Thieme, Ingrid B. Utne, Ali Mosleh, *A generic approach to analysing failures in human – System interaction in autonomy*, 129 SAFETY SCIENCE (2020).

overly rely on AI decisions and miss the need for intervention. AI systems perform diverse tasks in various environments, which makes it difficult for users to detect and understand possibilities of error, and to regain control when necessary.[68]

The users should be informed and aware of possible errors in the AI system. Consumers must be informed about all capabilities and disabilities of AI.[69] Regulatory standards should be in place for AI-enabled products to set accurate user expectancies and ensure ethical promotional practices. This includes providing explicit cautions and protective labels to enhance user awareness and promote the safe use of autonomous products.[70]

To ensure proper oversight of AI systems, users should understand the system's capabilities and limitations, enabling them to monitor performance and spot potential issues. They must be aware of risks, including automation bias, and know when to disregard, override, or halt AI outputs. Oversight measures should mitigate risks to health, safety, or rights, aligned with the system's risk level, autonomy, and context.[71] Users need to grasp AI product capabilities, stay alert to automation bias, accurately interpret outputs, and intervene when necessary. These requirements could extend the product liability regime under the CPA. [72]

Such measures will enhance consumer awareness of AI systems, safeguarding their right to informed use. This approach will minimise reliance on AI, reducing potential harm and producer liability, thereby fostering a healthier market.

---

[68] *Supra* note 39.

[69] Consumer Protection Act, 2019, § 2(9)(vi), No. 35, Acts of Parliament, 2019 (India).

[70] Kees Stuurman, Eric Lachaud, *Regulating AI. A label to complete the proposed Act on Artificial Intelligence*, 44 COMPUTER LAW & SECURITY REVIEW (2022).

[71] Artificial Intelligence Act, 2024, Art. 14, Reg. (EU) 2024/1689 of European Parliament and of the Council, 2024 (European Union).

[72] Consumer Protection Act, 2019, § 81(1)(e), No. 35, Acts of Parliament, 2019 (India).

E. Liability for harms

AI-enabled products differ significantly from normal products, necessitating tailored laws. The CPA promotes responsible marketing, but in the age of AI, it must prevent manufacturers from escaping liability through narrow definitions. AI products' unique nature requires broader definitions to hold manufacturers accountable for design flaws, system defects, and safety issues.[73]

For foreseeable harms, there should be specific requirements, certifications, and assessments for AI products to clarify user responsibility. Manufacturers have specific obligations, but users also bear the responsibility for ensuring proper use.[74] Courts should consider both manufacturers' precautionary measures and users' efforts to follow precautions and warnings.[75]

Unforeseeable harms associated with autonomous AI products pose a challenge in fixing liability. Assigning the costs of harm to AI technology beneficiaries incentivises them to make optimal decisions about usage and deployment.[76]

In tort law, parties can be held strictly liable for unforeseeable autonomous actions, such as those of children or animals even when those autonomous actions are unforeseeable.[77] Similarly, both manufacturers and users of AI technology should be considered potential controllers, as both have opportunities to manage the AI's process. Since manufacturers cannot fully control the system once it leaves their

---

[73] Beatrice Adelakun, *Enhancing fraud detection in accounting through AI: Techniques and case studies,* 6(6) FINANCE & ACCOUNTING RESEARCH JOURNAL 978-999 (2024).
[74] Marilia Ramos, Christoph Thieme, Ingrid Utne, Ali Mosleh, *A generic approach to analysing failures in human – System interaction in autonomy*, 129 SAFETY SCIENCE (2020).
[75] *Supra* note 50.
[76] Philipp Hacker, *The European AI liability directives – Critique of a half-hearted approach and lessons for the future,* 51 COMPUTER LAW & SECURITY REVIEW (2023).
[77] Behrens v. Bertram Mills Circus, Ltd. [1957] 2 Q.B. 1, 22.

custody, imposing liability will force them to improve safety testing before release and ensure updates thereafter. [78]

F. Stratified Consumer Protection Laws

In the contemporary context, there is a pressing need to stratify existing consumer protection laws to address the growing concern of consumer exploitation through the unethical use of AI. The law must evolve to not only impose stringent penalties on offenders but also serve as a robust deterrent against AI-related malpractices.

There is an urgent need to classify consumer exploitation as a form of consumer crime and introduce a specific legal framework that encompasses the misuse of AI technologies. Such legislation should differentiate between compoundable and non-compoundable offences as well as cognizable and non-cognizable consumer crimes, taking into account the varying degrees of exploitation. Provisions must be made for the imposition of severe penalties based on the gravity of the offence to ensure justice and deterrence.[79]

Additionally, for the efficient administration of justice, it is imperative to sensitize the judiciary to the potential misuse of AI technology, alongside its technical intricacies. This would facilitate more informed and expedited adjudication of cases involving AI exploitation. Training programs could be introduced for judges to enhance their understanding of AI-related issues, thus enabling them to make well-reasoned and timely decisions.

Furthermore, law enforcement, particularly those responsible for consumer protection, must undergo specialized training to effectively detect and investigate AI-related consumer crimes. A specialized division within consumer courts, dedicated to

---

[78] Miriam Buiten, Alexandre de Streel, Martin Peitz, *The law and economics of AI liability*, 48 COMPUTER LAW & SECURITY REVIEW (2023).

[79] Rajesh Bahuguna & Radhey Shyam Jha, *Age-Old Tools and Techniques to Protect Consumers Need to Be Sharpened in the Light of Artificial Intelligence*, 10 INTERNATIONAL JOURNAL ON CONSUMER LAW AND PRACTICE (2022).

handling AI-related offences, could also be established. This would expedite the resolution of such cases and contribute to the overall efficiency of the justice system.

VI. CONCLUSION

In today's economy, the integration of AI is essential for businesses to remain competitive. AI not only fosters business growth but also significantly enhances consumer experiences. However, the rise of AI and its complex algorithms has led to malpractice by digital platforms. The continuous collection of vast amounts of non-personal data can erode consumers' freedom of choice, as they may be subtly guided by sellers.

To safeguard consumer rights in the digital age, policymakers must regulate the collection and processing of observed data, which current laws inadequately address. Consumers should be informed about how their data is used, enabling them to make genuinely free and informed choices. Regulating data collection practices is a crucial first step in recognizing the need for further measures in the AI era. And the unregulated nature of data collection contract and ignorance towards 'observed data' is major source behind this disturbance, which is required to be regulated as first step to recognise the need of additional measures in AI-age.

AI-enabled products are becoming more prevalent. While automated machines are not new, the challenge arises when these machines on their own intelligence with no or minimal human intervention and cause harm. Current laws do not adequately address AI's liability or design defects. There is a pressing need to introduce safety provisions and certification procedures, similar to the EU model, to protect consumers. Additionally, consumer awareness regarding AI-enabled products that require human oversight is vital to alleviate manufacturers' liability. Moreover, in cases of unforeseeable damages, the strict liability principle in tort law effectively safeguards consumers.

Conclusively, Indian laws are evolving but proportionally slower than the growth of technology. Precaution of not being a burden on businesses with additional compliances is the main intention behind slow growth. Such an approach is indeed required for a developing economy but the market is a two-sided phenomenon, where consumers are there on another side. A healthy market can only exist when consumer rights are effectively protected.

HYPER-PERSONALIZATION IN INSURANCE VIS-À-VIS DATA PRIVACY

- AANCHAL AGARWAL & KUHU SRIVASTAVA

ABSTRACT

This paper investigates the revolutionary possibilities of hyper-personalisation in the insurance business, while also addressing fundamental issues surrounding data privacy. Hyper-personalisation, which uses real-time data and advanced analytics to deliver customised insurance solutions, offers several benefits, including higher customer retention, increased sources of revenue, and better risk management. This approach enables insurers to go beyond standard segmentation and provide 'segment-of-one' services, thereby improving the client experience. However, this technique for collecting client data creates significant privacy issues. This paper uses the doctrinal method, examining the existing and upcoming legal provisions on the regulation of data usage, and analyses the provisions under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, the Guidelines on Information and Cyber Security for Insurers, and the Digital Personal Data Protection Act, 2023 to look at how insurers must make ethical use of consumer data and whether these provisions find that elusive balance between protecting privacy and exploiting data.

Keywords: Hyper-personalisation, Insurance, Data Privacy, DPDP Act, IRDAI, IT Act.

I. INTRODUCTION

The Indian insurance sector is an industry that is constantly advancing. According to Invest India, this industry can easily surpass the $200 billion threshold by 2027[1]. India holds the ninth and fourth largest positions in the global market in the Life Insurance and other insurance sectors, respectively[2]. The country has come a long way since its first insurance establishment, which focused solely on life insurance in 1818. The opening of Oriental Life Insurance Company in present-day Kolkata marked the emergence of life insurance in India. Thereafter, the year 1850 marked the inception of the Triton Insurance Company Ltd. to cover the general insurance needs of the local public. Fast forward to the late 1990s and early 2000s, with the increasing growth of the insurance sector, the need for establishing a separate statutory body to oversee and boost the industry was deemed imminent. Ultimately, in April 2000, the Insurance Regulatory and Development Authority of India was formulated to regulate and develop the insurance industry[3]. With the advent of the twenty-first century, society experienced a vast technological shift that altered the consumer's needs in diverse ways. Everything has become exponentially internet-reliant, and people can access the internet with just a few clicks. As the concept of customised social media advertising and other techniques became increasingly popular among the masses, and people got accustomed to the idea of personalised goods and services, the insurance sector also picked up the notion of personalisation to become more customer-centric as the years passed. Today, more so after the Covid-19 pandemic, the prioritisation of comfort by individuals has propelled digital adoption leading to the generation of mass data and an increased use of behavioural data in organisational decision-making[4].

---

[1] Invest India, Department of Industrial Policy & Promotion, Ministry of Commerce and Industry, Government of India, *Insuring India, available at* https://www.investindia.gov.in/sector/bfsi-insurance (last visited on Aug. 28, 2024).

[2] *Id.*

[3] Evolution of Insurance in India, Insurance Regulatory and Development Authority of India, *available at https://irdai.gov.in/evolution-of-insurance* (last accessed Feb. 09, 2025).

[4] Wipro, Hyper Personalisation in Financial Services - A Wipro Report 4, (last accessed on January 14, 2025).

II. THE CONCEPT OF HYPER-PERSONALISATION

In an ever-evolving digital ecosystem, customer-centricity has become a *sine qua non* for entities seeking to carve a niche. Customer-centricity, though not a new concept, has a new-found meaning by virtue of hyper-personalisation. It is the way brands tailor their marketing services according to individual customer needs. It often means how "*…companies can send highly contextualized communications to specific customers at the right place and time, and through the right channel*"[5].

Previously, the focus rested on historical data, such as browsing and order histories, to customize products and experiences for customers. However, with the advent of hyper-personalisation, harnessing real-time data has taken centre stage.

At the heart of customer-centricity, and therefore, hyper-personalisation, lies prescience. The ability to understand and anticipate customers' needs is what makes hyper-personalisation unique and indispensable. Targeted, precise, and deeply contextual customer experiences are created by having real-time data analysis and artificial intelligence ("**AI**") work in tandem. Communication with customers rooted in segment-of-one ensures that messages are relayed at effective times and through effective platforms.

With digital marketing becoming increasingly competitive, hyper-personalisation ensures purposeful interaction with prospective customers and solidification of the existing customer base which in turn provides thrust to brand loyalty, thereby assuring the effectiveness of marketing campaigns.

---

[5] Deloitte. Connecting with meaning - *Hyper-personalizing the customer experience using data, analytics, and AI*, 8, *available at* https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-en-omnia-ai-marketing-pov-fin-jun24-aoda.pdf (last accessed on 14 Jan. 2025).

A. *Hyper-Personalisation in the Insurance Sector*

The insurance sector, competitive as it is, requires insurers to stand out and differentiate their products from the rest. The data set to be generated over the next three years is estimated to exceed the data begotten in the last thirty.[6] Accessing and utilizing this data aids insurers in understanding and prioritizing clients' needs while simultaneously adapting their products to cater to them. Real-time data comprising intricate, and often intimate details of customers acquired through smart wearable and internet of things ("**IoT**") devices is crucial in personalizing offerings for customers and concurrently attempting risk-specific underwriting. An example of this can be found in a project by Western India Palm Refined Oils Limited ("**WIPRO**")[7], where they worked with an Australian insurance provider to develop a risk-score allocating algorithm based on people's driving behaviour. This led the insurance provider to use the data to identify problem areas and offer discounts and higher premiums to drivers with superior or inferior risk scores, respectively.

The first and the most crucial step towards implementing hyper-personalisation is building a depository of customer data that can be used to create a precise and detailed profile. However, there is one other aspect of data collection that goes a long way in hyper-personalizing products and services for customers – ancillary data from insurance ecosystems[8].

An insurance ecosystem is one where multiple entities from within and outside of the industry work cohesively to develop, build, and deliver additional relevant products and/or services along with a central insurance offering. Insurance ecosystems are

---

[6] Adam Wright, *Worldwide IDC Global DataSphere Forecast, 2024–2028: AI Everywhere, But Upsurge in Data Will Take Time* (May 2024), *available at* /https://www.idc.com/getdoc.jsp?containerId=US52076424 (last accessed on Aug. 24, 2024).

[7] Suzanne J. Dann, *Hyper-personalisation: A Data-Driven Customer Engagement Model* (July 2021), *available at https://www.wipro.com/blogs/suzanne-jdann/hyper-personalisation-a-data-driven-customer-engagement-model/* (last accessed on Aug. 24, 2024).

[8] *Ibid.*

relevant because they access and utilize data from multiple sources to form a customer profile so precise that hyper-personalisation happens organically and on a scale that entities that are purely risk-cover providers cannot reach. A motor vehicle insurer offering assistance after accidents, repair works, and vehicle replacements is an example of an insurance ecosystem.

Onsurity[9] is a company that primarily offers group health insurance but has the provision of health membership, a holistic product that includes health check-ups and medicines at discounted prices, consultation with doctors over text, phone calls, and video, an insurance claim concierge service, and a fitness membership where google fit or the apple health app can be downloaded and linked with their app for an integrated and seamless experience. This differs from traditional insurance providers in that personalisation is limited to a choice between pre-determined plans, and add-on benefits such as critical illness coverage or maternity benefits. The scope for customisation is less, as is the emphasis on data-driven insights.

As might be expected, Onsurity has the opportunity to gather data from all ancillary service providers and assimilate it into its own to deliver a hyper-personalised experience to its customers, both existing and potential. Ecosystems also promote supplementation of coverage and policy renewals, often collecting and using data and customer feedback to create mutually beneficial products and services.

B. *Benefits of Hyper-Personalisation*

Ultimately, hyper-personalisation's benefit is creating and configuring insurance offerings that have increased marketability and sustainability. The benefits of hyper-personalisation can be categorised into the following:

[9] OnSurity, About Us, *available at* https://www.onsurity.com/about-us/ (last accessed Jan. 14, 2025).

i. Customisation of Offerings

Real-time data collection leading to tailor-made and individualistic insurance offerings has three-fold benefits. At the marketing stage, it positively impacts the conversion rate, in that the chances of ad clicks converting into product/service purchases or any other desired outcome increase[10]. The second benefit is customer retention because a product designed with the specific needs of individuals in mind is inherently sustainable.[11] Lastly, ecosystems with relevant ancillary data help maintain relevancy throughout the life of the product. Sustainable offerings also reduce the risk of policy surrender and lapse, thus saving customers and insurers from financial loss. A recent example is the revision in the exit payout policy on life insurance products[12] before which life insurance holders did not get any surrender value in the first year.

ii. Revenue Maximisation and Cost Minimisation

Content and offerings are driven by data, increasing click-through and conversion rates and, therefore, increasing revenue generation. Dynamic pricing, defined as "*a strategy that bases products or services' prices on evolving market trends, such as supply and demand, competitor pricing, and inventory levels*[13]" ensures that after potential high-risk customers are identified, premiums or discounts are offered accordingly. Acquisition and retention costs are also reduced through the use of tailored offerings. Digital platforms use data analytics and technologies like artificial intelligence and machine

---

[10] Go4Customer (@Go4Customer), *The Rise of Hyper-Personalization in BPO Services* (Oct. 26, 2023, 10:00 AM), *available at* https://www.linkedin.com/pulse/rise-hyper-personalization-bpo-services-go4customer-krfkc?trk=organization_guest_main-feed-card_feed-article-content (last accessed Feb. 13, 2025).

[11] *Ibid.*

[12] The Insurance Regulatory and Development Authority of India, Master Circular on Life Insurance Products, IRDAI/ACTL/MSTCIR/MISC/89/6/2024 (Issued on June 12, 2024).

[13] Harvard Business School, Dynamic Pricing: What It Is & Why It's Important, *available at* https://online.hbs.edu/blog/post/what-is-dynamic-pricing (last accessed Jan. 14, 2025).

learning to deploy sophisticated algorithms that analyse market conditions and predict optimal pricing.[14]

iii. Elevation of Customer Experience

Hyper-personalised marketing ensures real-time customer segmentation or a step further, a segment-of-one, and often round-the-clock customer service. Dynamic landing pages are also an important part of hyper-personalised marketing aimed at simplifying the journey of customers. These are "…*customized landing pages that allow businesses to tailor their content and messaging for each specific user. They use data such as location, device type, search query and browsing history to craft a highly-relevant page for each visitor.*"[15] Personalised services, on the other hand, also distinguish insurers from the hoard and capture the attention of customers. Focused and empathetic treatment of each customer in a sea of existing and prospective clients paves the way for a satisfying customer experience.

---

[14] *Ibid.*

[15] Wix, *Dynamic Landing Pages*, WIX ENCYCLOPEDIA, *available at* https://www.wix.com/encyclopedia/definition/dynamic-landing-pages (last accessed Feb. 13, 2025).

C. Challenges of Hyper-Personalisation

Undoubtedly, hyper-personalisation has proven to be, *inter alia,* a boon for insurance companies by boosting their revenue and maximising client engagement. This technique has also been fruitful for consumers, as the delivery of tailored insurance services catering to their tastes solves all their concerns and fulfils all their demands in one go. However, numerous difficulties are associated with the implementation, and facilitation of hyper-personalisation in the insurance sector.

i. Transparent and Ethical Usage of Data

Hyper-personalisation imposes a massive burden on insurers to maintain transparency and ethicality when utilising clients' personal and vital data. Companies need to pose ethically by acquiring the due consent of clients before data collection and employment to provide hyper-personalised services. They should further provide detailed insight regarding the modes of collection and data usage methods so that the clients remain aware of exactly how their data is being sourced and where it is being used[16]. The insurers must hand a way out to the clients if one does not wish to avail of hyper-personalised services at the cost of their personal data[17].

ii. Quality and Accuracy of Data

Data collected is only as authentic as its source. Companies must ensure they collect data from trustworthy sources; otherwise, it becomes difficult to ascertain its accuracy. Insurers must ensure that their AI systems employed to collect, process[18], and utilise data are free from bias otherwise, the results will be inefficient. Additionally, if the

---

[16] Sowmya Siddalinganagowda Patil, *Challenges in Hyper-Personalization*, INFOSYS BLOGS (Oct. 26, 2023), *available at* https://blogs.infosys.com/digital-experience/emerging-technologies/challenges-in-hyper-personalization.html (last accessed Feb. 13, 2025).

[17] Leander Fernandes, Hyper-Personalisation in Insurance – Key to Meet & Exceed Customer Expectations, Anaptyss, *available at* https://www.anaptyss.com/blog/hyper-personalisation-insurance-meet-exceed-customer-expectations/ (last accessed Jan. 14, 2025).

[18] *Ibid.*

data proves unauthentic or prejudiced, the successful implementation of hyper-personalisation cannot be guaranteed.

iii. Complex Implementation Procedure

Implementing hyper-personalisation in a manner that helps insurers reap its benefits is a highly taxing process. Effective and strategic implementation involves hiring professionals with significant knowledge of such procedures and even upskilling them to ensure they are up-to-date with recent trends. If needed, insurers have to join forces with other companies involved in delivering relevant services[19] that are closely associated with the kind of insurance dealt with by the insurers.

iv. Added Costs

While hyper-implementation ultimately shoots up insurance companies' revenue, it can turn out to be an expensive exercise. This procedure requires state-of-the-art software[20], as insurance companies need to set up a repository that stores and processes all clients' vital data. Hyper-personalisation necessitates seamlessly integrating software tools, such as Customer Relationship Management systems, specialized personalisation engines, AI-powered analytics platforms, and marketing automation softwares. These elements function in harmony, facilitating the real-time acquisition and analysis of customer data. This comprehensive framework empowers businesses to tailor customer experiences across all touchpoints, including websites, emails, and mobile applications, ensuring alignment with unique preferences, and behavioural patterns of each individual. Building or procuring such software can be a heavy burden, especially for new companies. Moreover, added costs are associated

---

[19] El Khalfi, *Challenges Implementing Hyper-Personalized Marketing: How to Overcome Them*, LINKEDIN (Jan. 17, 2024), *available at* https://www.linkedin.com/pulse/challenges-implementing-hyper-personalized-marketing-how-el-khalfi-b3yce (last accessed Feb. 13, 2025).

[20] Andrew Pearson, Personalisation the artificial intelligence way, 10 J. GLOBAL RES. 7331, 245-46 (2020).

with employing seasoned professionals who are experts in such work and can promise optimum results to the insurers.

v. Privacy Regulations

The insurance companies must mandatorily comply with data privacy laws applicable to them. Additionally, keeping in mind the growing threat of data breaches and cybercrimes, insurers need to equip themselves with effective systems to tackle such cyber threats, as customers' personal data is at risk.

III. RIGHT TO PRIVACY AND DATA PROTECTION IN INDIA

The fundamental rights provided under Part III of the Constitution of India guarantee the right to life and personal liberty under Article 21[21]. The nine-judge bench unanimously, but through six separate concurring opinions in the case of Justice K.S. Puttaswamy v. Union of India[22], stated,

> *"The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."*

The judgment overruled two previous ones that dealt with the same matter but disagreed with the idea of privacy being a fundamental right. The overruled cases were the MP Sharma v. Satish Chandra[23], and Kharak Singh v. State of Uttar Pradesh[24]. The Puttaswamy case also highlighted the dire need for a new data privacy code.

The parliament of India passed the Digital Personal Data Protection Act, 2023 (**"DPDP"**)[25] which received presidential assent on the 11th August, 2023. The main intention behind this act was to address and comply with the Puttaswamy judgment and formulate an act that performs a dual role, i.e., acknowledges the right to privacy

---

[21] India Const. art. 21.
[22] (2017) 10 SCC 1.
[23] (1954) 1 SCC 385.
[24] (1954) 1 SCC 385.
[25] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

of all citizens, and simultaneously the need to collect data for conducting processes that are lawful and within the ambit of the Act. Before the enactment of the DPDP Act, the data privacy issue was dealt with by the Information Technology Act, 2000[26] ("**IT Act**"), and its associated rules, i.e., the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[27], commonly referred to as the IT Rules (**"SPDI Rules"**).

A. Insurance Hyper-Personalisation In The Light Of Data Privacy

Hyper-personalisation, though revolutionary, poses significant data privacy concerns. Adhering to data privacy and protection norms while providing hyper-personalised products and services becomes a balancing act, which, while being arduous, is achievable. This can be done by ensuring transparency in data collection, storage, and use, using anonymisation and pseudonymisation techniques, and obtaining consent, including the right to correct, update, and delete data. Ensuring adequate safety measures for storing data is another way of preventing breaches and misuse.

For instance, the IRDAI (Maintenance of Insurance Records) Regulations, 2015[28], in Regulations 3(3)(b) and 3(9), lays down that insurers should ensure the presence of all necessary security features in the system hosting policy and claims records[29], and that all such records for policies issued, and claims made in India are held in such data centres as are located and maintained in the country itself[30].

Similarly, Regulation 12 of the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017[31] ("**Outsourcing Regulations**") provides that it is the duty of insurers to make certain, with respect to outsourcing service providers, that they have

---

[26] Information Technology Act, 2000, No. 21, Acts of Parliament, 2023 (India).
[27] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
[28] IRDAI (Maintenance of Insurance Records) Regulations, 2015.
[29] IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3(3)(b).
[30] IRDAI (Maintenance of Insurance Records) Regulations, 2015, Reg. 3(9).
[31] IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, Reg. 12.

the resources to secure the information of policyholders, the information provided to them remains confidential, and that once data has been retrieved, they cannot access or use it.

These regulations are especially relevant when InsurTech companies and insurance ecosystems are steadily taking over the market. It is imperative that each entity in an ecosystem is equally regulated to prevent data leaks.

i. Information and Cyber Security Guidelines 2017 and 2023

The IRDAI, in 2017, published Guidelines on Information and Cyber Security for Insurers[32] ("**CS Guidelines**") to ensure that the regulated entities implemented procedures guaranteeing the confidentiality of data. CS Guidelines applied to all data held and maintained by insurers and third-party vendors. As with the Outsourcing Regulations[33], insurers have an obligation to ascertain that, if policyholder information is shared with intermediaries, there are checks in place to deal with any cyber security or information issues that might arise.

IRDAI, recognizing the importance of securing data throughout its lifecycle, from creation, storage, and use to rest and destruction, laid down a comprehensive framework wherein organisations would:

First. Classify data as critical and non-critical and devise a system to secure critical data;

Second. Obtain undertakings from all entities with access to critical data for maintaining confidentiality;

Third. Take approval from information holders/business owners if sensitive data is to be outsourced; and

[32] Information and Cyber Security for Insurers, 2017.
[33] *Supra* at 26.

Fourth. Ensure that mechanisms are in place for the effective destruction of data stored.

These guidelines also required insurers and their intermediaries to comply with statutory provisions dealing with information and cyber security including the SPDI Rules.

Digitisation provided impetus to the IRDAI to replace the 2017 CS Guidelines with the Insurance and Cyber Security Guidelines of 2023[34] ("**CS Guidelines 2023**") that focus on the security of data instead of simply securing the systems that store it. The need to amend the 2017 guidelines was felt imminent due to the growing facilitation of all services digitally, fuelled by the 2020 pandemic, which led to the world relying heavily on remote-based frameworks for conducting business and occupation.

A notable change is that its applicability has been stretched significantly, as earlier 2017 guidelines applied only to insurers, but now it applies to numerous entities collectively referred to as 'Regulated Entities'. The guidelines also state that Regulated Entities while sharing data with third parties and their personnel, must employ a risk-focused technique, use relevant precautions to safeguard data, and shield against cybercrime, especially client's data being lost, misused, or breached in any manner.

The CS Guidelines 2023 made it mandatory for Regulated Entities to formulate and adhere to a governance framework that shall include a board of directors, and committees such as a risk management committee, and security risk management committee[35]. The main role of this constituted organisation would be to strategically employ practices and oversee data security. These guidelines also make it compulsory to formulate numerous internal committees with distinct roles and responsibilities for each committee and its members[36].

---

[34] Insurance and Cyber Security Guidelines, 2023.
[35] Insurance and Cyber Security Guidelines, 2023, Guideline 1.6.
[36] *Ibid.*

The CS Guidelines 2017 only mentioned that a particular organisation's 'acceptable-use policy' must include social networking sites but did not provide anything in detail. The 2023 guidelines detail it by adding certain guidelines on acceptable use, including but not limited to how personnel should employ networking sites for business and personal gains. The 2023 guidelines further outline that personal use of social networking apps by workers cannot be construed as official corporate communications. Additionally, personnel cannot use such apps for business unless the organisation itself has green-signalled such usage and training has been provided to the worker if needed for such usage.

ii. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[37]

The privacy policy should be unambiguous, published on the insurer's website, and contain information about the type of data collected, and its intended use[38]. Consent for data collection should be taken in writing and information collected should be necessary and for a lawful purpose[39]. Additionally, people whose data is collected should know the following:

First. The fact that their data is being collected;

Second. The purpose of such a collection; and

Third. Details of collection and retention entities[40].

---

[37] *Supra* at 22.

[38] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 4.

[39] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5.

[40] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5(3).

Data providers should also be provided the right to review and amend the information provided[41], not provide the information sought, and withdraw consent[42]. Information collected by insurers shouldn't be retained for longer than required[43], and except in cases of information sharing with government agencies or compliance with legal obligations, permission of the information provider is needed before disclosing their information to any third party. While transferring data, it should be ensured that the transferee adheres to the same standard of data protection as the transferor, such transfer is necessary and unavoidable, and that the person whose data is to be transferred has agreed to such transfer[44].

iii. The Digital Personal Data Protection Act, 2023

The DPDP Act[45] applies to digital personal data and not to non-personal data. The act is currently not in force, but once it comes into force by the Central Government's notification, it is set to replace Section 43A of the IT Act, 2000, and the SPDI Rules. Section 4 explicitly states that the personal data of a data principal can be processed either by taking due consent, or for some legitimate reason[46]. Section 5 states that a request must be made to receive the consent of the data principal, and such a request can be made by sending out a clear, reasonable notice that shall mandatorily include the details and purpose of data collection, mode and manner of consent withdrawal, and lodging a complaint to the board[47].

---

[41] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5(6).
[42] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5(7).
[43] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 5(4).
[44] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 7.
[45] *Supra* at 20.
[46] Digital Personal Data Protection Act, 2023, S. 4.
[47] Digital Personal Data Protection Act, 2023, S. 5.

All the above-mentioned information, which must be included in the notice, is crucial for the data principal to make an informed decision before handing out the consent. Section 6(1) of the act necessitates that the consent be free, to the point, and unambiguous[48]. Sub-section (2) states that if the data principal has provided consent for something capable of breaching the provisions of this act, then the consent shall not apply to the extent of such breach[49]. Section 6(4) grants the data principal the power to withdraw consent at any time, provided the data principal is liable for all consequences arising out of such withdrawal[50]. Section 6(6) states that the data fiduciary must stop processing the personal data of the data principal as soon as practicable after the data principal withdraws the consent[51]. Sub-sections (7) and (8) grant the data principal the power to hand out, withdraw, or review consent via a consent manager who is approved by and registered with the data protection board, and such person shall be accountable to the data principal[52].

Moving forward, Chapter III of the DPDP Act, which contains Sections 11 to 15, deals with the rights and duties of a data principal. As per this chapter, the following rights have been provided to the data principal:

First. Right to access their personal data[53];

Second. Right to ask for correction in their data[54];

Third. Right to demand their data be erased[55];

Fourth. Right to nominate a person to handle such things in case of death or any sort of incapacity[56]; and

---

[48] Digital Personal Data Protection Act, 2023, S. 6(1).
[49] Digital Personal Data Protection Act, 2023, S. 6(2).
[50] Digital Personal Data Protection Act, 2023, S. 6(4).
[51] Digital Personal Data Protection Act, 2023, S. 6(6).
[52] Digital Personal Data Protection Act, 2023, S. 6(7)&6(8).
[53] Digital Personal Data Protection Act, 2023, S. 11.
[54] Digital Personal Data Protection Act, 2023, S. 12(1).
[55] Digital Personal Data Protection Act, 2023, S. 12(3).
[56] Digital Personal Data Protection Act, 2023, S. 14(1).

Fifth. Right to seek redressal and submit a grievance against data fiduciaries and consent managers[57].

Sixth. Additionally, the following duties have been mandated upon the data principals:

Seventh. They need to exercise their abovementioned rights within the ambit of applicable and relevant laws[58];

Eighth. They shall not impersonate another being for their benefit[59];

Ninth. Disclose all relevant information and not hide anything concerning providing data for documents, unique identifiers, or identity or address proof issued by the State or its instrumentalities[60];

Fourth. They must not file false grievances or take advantage of these complaint mechanisms[61]; and

Fifth. They must present only reliable and accurate data when demanding to alter or erase their personal data[62].

B. Interplay between the DPDP Act and the Insurance Sector

The newly formulated DPDP Act promises a noteworthy change in our country's data privacy regime, with significant and wide-ranging ramifications for numerous sectors, such as the insurance industry. Since the Indian insurance industry procures and manages a massive amount of personal data, the DPDP shall heavily govern this sector. With the implementation of this Act, it will become necessary for data fiduciaries to analyse and evaluate their current practices, including but not limited to the mode and manner of data handling and particularly confidentiality agreements

[57] Digital Personal Data Protection Act, 2023, S. 13.
[58] Digital Personal Data Protection Act, 2023, S. 15(a).
[59] Digital Personal Data Protection Act, 2023, S. 15(b).
[60] Digital Personal Data Protection Act, 2023, S. 15(c).
[61] Digital Personal Data Protection Act, 2023, S. 15(d).
[62] Digital Personal Data Protection Act, 2023, S. 15(e).

with third parties and vendors with whom they share users' data to provide services.[63] For instance, health insurers usually share consumers' data with third parties for numerous reasons, including sharing clients' medical histories, namely hospitals and clinics, for facilitation purposes[64].

Moreover, general or specific insurance companies employ several tele-calling, social networking, and other modes of connection with clients to provide information regarding lapse of policies or the status of claims. Such companies also utilise these communication techniques to obtain client feedback to ensure optimal quality service. Since the Act expressly mandates obtaining consent from clients and specifying the purpose and details of data collection if the purpose of data collection does not fall within 'legitimate uses[65]', after the due implementation of this Act, the data fiduciaries shall have to send out a detailed notice specifying all the reasons and purposes of data usage to their clients to seek their approval since most of the abovementioned instances and several others shall not necessarily fall within the ambit of 'certain legitimate uses' given under Section 7[66].

Additionally, regarding seeking consent, the insurance companies may have to alter or tweak their existing practice as it may not comply with the latest developments after implementing the DPDP Act. The requirement of presenting a notice for approval exists in SPDI Rules and Cyber Security Guidelines as well, but those mandates are not as detailed and thorough as the ones now present in the DPDP Act.

---

[63] Nishith Desai Associates, *India's Digital Personal Data Protection Act, 2023: History in the Making*, *available at* https://www.nishithdesai.com/information/news-details/india-s-digital-personal-data-protection-act-2023-history-in-the-making (last accessed Feb 13, 2025).

[64] Indranath Bishnu & Anirud Sudarsan R, *Policyholder Data Sharing in India – Time for a Consent-Based Regime?*, CORPORATE LAW BLOG (Aug. 18, 2022), *available at* https://corporate.cyrilamarchandblogs.com/2022/08/policyholder-data-sharing-in-india-time-for-consent-based-regime/#_ftnref16 (last visited Feb. 14, 2025).

[65] Digital Personal Data Protection Act, 2023, S. 7.

[66] *Ibid.*

IV. CONCLUSION

Privacy is an inherent right and thus means different things to different people. One meaning ascribed to privacy is control over outside access to information. This aspect of privacy is especially relevant in this day and age, where possessing personal information is not just about power, it is also about money. Digitalisation has opened a whole new world for businesses, from revamping business models such as the shift from insurance companies to insurance ecosystems to creating new value-adding and value-producing opportunities. Data from every aspect of our lives – food and sartorial choices, health concerns, conversations, and movements—is meticulously collected, scrutinised, and analysed to reach a conclusion, a digital profile so exact, it seems nothing less than divine providence.

Data usage, like any other coin, has two sides. One is a consensual, legitimate use, proportional to the objective it seeks to attain, while the other is a tool to do anything from a subtle nudge towards a particular offering to a campaign hoping to influence, manipulate, or even reshape individual decision-making. This potential diametric contradiction leads us to the issue of regulation.

The existing framework governing data privacy in insurance protects data throughout its lifecycle, especially with the revision of the CS Guidelines in 2023, which, along with the SPDI Rules covers all entities associated with the insurance process as well as in the insurance ecosystem through the provisions on transfer of data. The DPDP Act of 2023, however, has some loopholes. For instance, even though Section 8(6) mandates reporting breaches in data to the board, no timeline is mentioned for the same which can result in data fiduciaries withholding information and consequently evading penalty.

Similarly, the Act doesn't require data fiduciaries to obtain the consent of data principals for sharing their data with a third-party data processor. This not only

undermines the consent of the principal but also paves the way for unbridled data-sharing with multiple entities.

Since the DPDP Act is yet to be implemented, it cannot be said with absolute certainty how the existing framework of laws for the insurance sector will be impacted by it, however, the shortcomings of the Act underscore the requirement of a nuanced approach to data privacy to balance the sanctity of personal data and the need to leverage it.