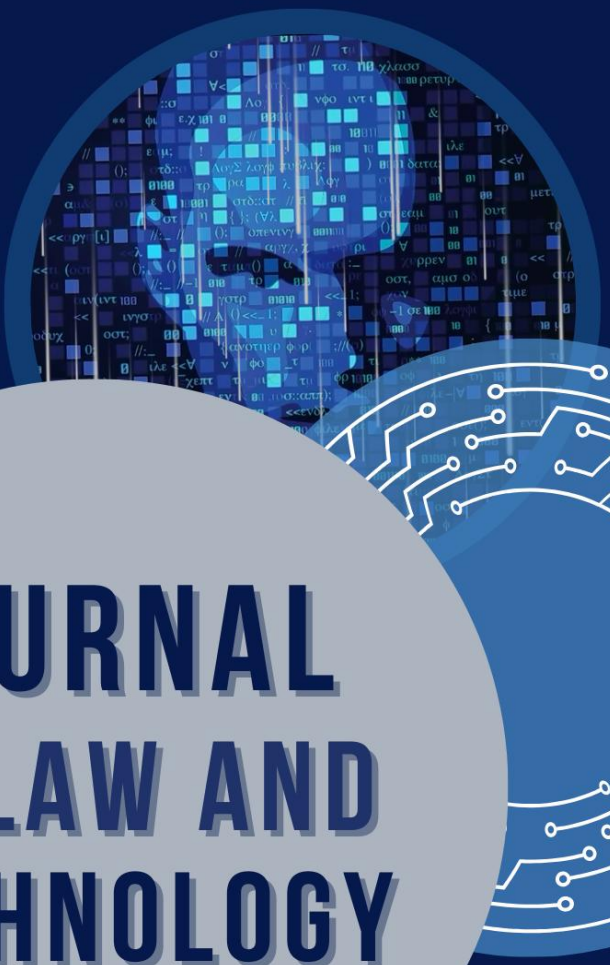
Cell for Law & Technology



JOURNAL OF LAW AND TECHNOLOGY

Volume I

2025

CELL FOR LAW AND TECHNOLOGY
IN COLLABORATION WITH RAJIV GANDHI NATIONAL CYBER LAW CENTRE, NLIU, BHOPAL ESTABLISHED BY THE MHRD (NOW THE MINISTRY OF EDUCATION) GOI, NEW DELHI

NLIU JOURNAL OF LAW AND TECHNOLOGY

VOLUME I

APRIL, 2025

NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

Kerwa Dam Road, Bhopal, India – 462 044 (Madhya Pradesh)

The NLIU Journal of Law and Technology is published by the Cell for Law and Technology (CLT) in collaboration with Rajiv Gandhi National Cyber Law Centre at National Law Institute University, Bhopal established by the MHRD (now the Ministry of Education) GOI, New Delhi.

The NLIU Journal of Law and Technology invites unsolicited manuscripts for publications. Such manuscripts should be submitted in MS Word (.docx format) to clt.editorial@nliu.ac.in. All citations and text conform to *Oscola (4th edn.)*.

Mode of Citation:

1 NLIU JLT (2025)

Published by:

The Registrar

National Law Institute University Bhopal

(M.P.) 462044 INDIA

STUDENT BODY OF THE JOURNAL

CONTENTS

MESSAGE FROM THE PATRON

- *Prof. (Dr.) S Surya Prakash*

It gives me immense pride to introduce the inaugural volume of the NLIU Journal of Law and Technology, an initiative by the Cell for Law and Technology at the National Law Institute University, Bhopal. The CLT has been a pioneer in fostering critical scholarship at the intersection of law and technology, addressing the challenges posed by rapid technological advancements through their blog. In an era where artificial intelligence, blockchain, biometric systems, and digital ethics are reshaping societal norms, the CLT serves as a vital platform for exploring how legal frameworks can adapt to these transformative changes while safeguarding public interest.

The articles featured in this inaugural volume reflect the diversity and complexity of this dynamic field. From an analysis of biometric privacy claims in India and the U.S. to critical discussions on fiduciary obligations in AI-driven corporate governance, this journal offers fresh perspectives on emerging challenges.

The advent of the Digital Personal Data Protection Act, 2023 has ushered in a new era for data regulation in India. As we witness the advent of digital law, Journal for Law and Technology is indispensable for shaping informed policy responses.

In conclusion, I extend my heartfelt congratulations to the editorial team, faculty advisors, authors, and all contributors who have made this endeavor possible. This journal is not merely an academic publication; it is a beacon for thought leadership in law and technology. I am confident that it will inspire meaningful dialogue among scholars, practitioners, and policymakers while serving as an invaluable resource for addressing the challenges of our digital age.

MESSAGE FROM THE FACULTY ADVISOR

- *Prof. (Dr.) Atul Kumar Pandey*

It is with immense pride that I introduce the inaugural volume of the *NLIU Journal of Law and Technology*. As the Faculty Advisor, I have had the privilege of overseeing every aspect of this endeavor from its conceptualization and naming to the editorial process, proofreading, and publication. The journal stands as a testament to the dedication and intellectual rigor of our student editorial team.

The rapid evolution of technology has brought about profound changes in society, presenting both opportunities and challenges for legal systems worldwide. This journal seeks to address these emerging issues by providing a platform for critical scholarship on topics ranging from data privacy and artificial intelligence to digital ethics and regulatory frameworks. The articles in this volume reflect the diversity and complexity of these subjects, offering insights that are both timely and impactful.

The journey to this publication has been one of collaboration and learning. The student editors have demonstrated remarkable commitment, engaging in meticulous research, rigorous editing, and thoughtful curation of content. Their efforts have ensured that this journal meets the highest standards of academic excellence.

As we present this first volume, I am reminded of the broader mission that underpins this initiative: to contribute meaningfully to the discourse on law and technology while nurturing a culture of intellectual curiosity and critical thinking. It is my hope that this journal will not only serve as a repository of knowledge but also inspire future scholarship in this dynamic field.

I extend my heartfelt congratulations to the editorial team, authors, and everyone who has supported this endeavor. May this journal continue to grow in stature and impact, becoming a beacon for thought leadership in law and technology.

EDITORIAL NOTE

— Rishita Sethi & Hussain

The *NLIU Journal of Law and Technology* is proud to present its inaugural volume, marking a significant milestone in the exploration of the intersection between law and technology. As a publication of the Cell for Law and Technology at the National Law Institute University, Bhopal, this journal aspires to serve as a dynamic platform for rigorous academic discussions that address contemporary challenges and opportunities arising from technological advancements within legal frameworks.

In an era defined by rapid technological evolution where artificial intelligence, data privacy, digital ethics, and regulatory frameworks are reshaping societal norms, the journal seeks to bridge the gap between legal scholarship and technological innovation. This volume features a diverse array of articles that delve into critical issues such as biometric privacy, AI governance, deepfake regulation, data protection laws, and the ethical implications of emerging technologies.

The editorial team has worked diligently to uphold the highest standards of academic integrity and quality. The articles included in this volume were selected through a rigorous review process to ensure their relevance, originality, and scholarly rigor. We extend our heartfelt gratitude to our esteemed patrons, faculty advisors, contributors, and the dedicated student editorial team whose collective efforts have brought this vision to fruition.

As we embark on this journey, we hope that this journal will not only enrich academic discourse but also inspire meaningful dialogue among policymakers, practitioners, and scholars. It is our sincere aspiration that the *NLIU Journal of Law and Technology* will contribute significantly to shaping the future of law in an increasingly digital world. We invite readers to engage with the ideas presented in this volume and join us in advancing scholarship at the nexus of law and technology.

REVISITING DATA PRIVACY CONCERNS OVER WORLDCOIN FOR INDIA: REGULATION, CONSENT, DATA TRADE AND FUTURE IMPLICATIONS

—Sharanya Chowdhury[*]

ABSTRACT

This paper seeks to delve into the nuances of the Worldcoin ban and its cause, particularly focusing on the resurfacing of data privacy concerns. The Kenyan, Portuguese and Spanish bans present 3 critical reasons why such a venture might be a step too far into the future. This research aims to shed light on the pressing need for robust (sensitive) personal data privacy laws and mechanisms for informed consent and the future course of action in India. Further, it presents a critical analysis of the company's approach to introducing biometric authentication to a bulk of nations in light of the Kerfuffle around the ban.

Keywords: *Fintech, Cryptocurrency, Data Privacy, Biometrics, Worldcoin, TMT Law, Digital Personal Data Protection Act 2023, Technology Law, Data Privacy Law.*

INTRODUCTION

Worldcoin has emerged as a significant player in the ever-expanding universe of cryptocurrencies, promising a novel approach to digital currency distribution. Unlike traditional cryptocurrencies, Worldcoin aims to achieve widespread adoption through a unique mechanism that involves distributing its tokens to individuals worldwide. This ambitious vision, coupled with its innovative distribution model, has garnered attention from both enthusiasts and sceptics alike. Worldcoin seeks to revolutionize the way cryptocurrencies are disseminated, envisioning a more equitable and inclusive global financial system. By offering

[*] The author is a student at Dr. Ram Manohar Lohiya National Law University (RMLNLU).

tokens directly to individuals, rather than through mining or trading, it aims to democratize access to digital assets and promote financial empowerment on a global scale.[1]

Blockchains are heavily affected by bots, with a large scale of transactions being automated. While some are legitimate, many, like airdrop farming bots, cause network congestion and high fees, especially on chains optimized for low fees and high throughput.

The project is led by OpenAI CEO Sam Altman and is supported by organizations like the Worldcoin Foundation and Tools for Humanity.[2] To effectively differentiate them from bots or artificial intelligence.[3] Following the validation of their World ID using an "Orb" device, individuals gain access to a Worldcoin cryptocurrency wallet, enabling them to acquire the WLD token. This token not only offers utility but also confers governance rights. World Chain attempts to tackle this using World ID, allowing users to anonymously verify their humanity through zero-knowledge proofs. Similar to how World ID is used on platforms like Discord, users can verify their blockchain addresses without linking them to their identity, receiving a 'blue checkmark' of verification.

However, as with any disruptive technology, Worldcoin's journey has been met with its fair share of scrutiny and challenges. The recent ban imposed by Spain has cast a spotlight on the project, raising questions about its compatibility with existing regulatory frameworks and concerns regarding data privacy. In a recent development that has sent ripples through the global cryptocurrency community, Spain has made the bold move to temporarily ban Worldcoin, citing profound concerns over data privacy.[4] In response to this, Sam Altman has filed a lawsuit to object to the same, resulting in a battle of the lawsuits.[5]This has reignited a crucial debate surrounding the intersection of emerging technologies, individual liberties, and regulatory oversight.

[1]'Frequently Asked Questions' (*Worldcoin*) <https://worldcoin.org/faqs> accessed 9 May 2024.
[2]Curry B, 'Worldcoin: The Cryptocurrency That Wants to Scan Your Eyeballs' (*Forbes*, 15 August 2023) <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-worldcoin> accessed 9 May 2024.
[3]Eye on Tech, 'What Is Worldcoin? An Introduction' (*YouTube*, 12 October 2023) <https://www.youtube.com/watch?v=b28K6prjoP8> accessed 9 May 2024.
[4]Pinedo E and Howcroft E (*Spain's High Court upholds temporary ban on Worldcoin Iris-scanning venture | Reuters*, 12 March 2024) <https://www.reuters.com/technology/spains-high-court-upholds-temporary-ban-worldcoin-iris-scanning-venture-2024-03-11/> accessed 9 May 2024.
[5]'Sam Altman's Worldcoin Files Lawsuit after Spanish Ban' (*The Economic Times*, 8 March 2024) <https://economictimes.indiatimes.com/tech/technology/sam-altmans-worldcoin-files-lawsuit-after-spanish-ban/articleshow/108334931.cms?from=mdr> accessed 9 May 2024.

A. Explicit Ethical Conundrum

At the heart of the Worldcoin ecosystem lies the World ID system, a pivotal component meticulously crafted to offer a secure and privacy-centric method of user identification within the network.[6] The primary goals of the World ID system extend beyond mere identification; they are aimed at robust fraud prevention. The Company's dependency on AI for verifying the "humanness" of transactions highlights the critical importance of accurate data and genuine human input validation.[7] In this context, WorldID serves as a pivotal countermeasure against AI-driven misinformation by authenticating human users through the distinct biometric characteristics of their iris.[8] This innovative approach ensures unmatched precision in transaction verification, effectively thwarting fraudulent activities.

The ethics behind sensitive data collection is straightforward in its aim but not its execution. However, the security web required to realise these goals is a complex one, especially when companies seek to utilize almost-uniform policies in countries with contrasting cultural and economic realities. In this paper, we seek to understand whether this is a sound approach and whether the company is structurally prepared to take on the huge goal it has set its eyes on.

It's crucial to clarify that the intent of this research isn't to single out Worldcoin as the exclusive issue within this context. Worldcoin simply forms a case study. Biometric authentication, lacking a regulatory framework, poses inherent dangers, regardless of the entity implementing it. For instance, Amazon One, a palm authentication payment system, has already been deployed.[9] What makes this particularly alarming is its potential to become a ubiquitous payment method, possibly even for everyday transactions like purchasing a Starbucks coffee.

B. Concerns in Spain and the EU

Concerns in Spain were mainly regarding the complaints received by the Spanish Data Protection Agency (AEPD, Spanish: Agencia Española de Protección de Datos) regarding the

[6]Hetler A, 'Worldcoin Explained: Everything You Need to Know' (*WhatIs*, 9 August 2023) <https://www.techtarget.com/whatis/feature/Worldcoin-explained-Everything-you-need-to-know> accessed 9 May 2024.
[7]Rodrigues de Oliveira Habib Pereira N, Nelson Elias C and Souza B, 'ImplantesDentários de Pequenos DIÂMETROS – Uma Análise' [2023] Ciência e Tecnologia dos Biomateriais.
[8]Sehrawat JS and Sankhyan D, 'Iris Patterns as a Biometric Tool for Forensic Identifications: A Review' (2016) 5 Brazilian Journal of Forensic Sciences, Medical Law and Bioethics 431.
[9]DeVon C, 'Amazon Will Soon Let You Pay for Groceries with Your Palm at Any Whole Foods-but Tech Experts Urge Caution' (*CNBC*, 26 August 2023) <https://www.cnbc.com/2023/08/26/amazon-biometric-payments-privacy-concerns.html> accessed 9 May 2024.

non-consensual data collection with a lack of information being supplied on how such information is being used along with a lack of differential treatment of sensitive (biometric) data.[10] To which Worldcoin claimed that the Spanish authorities were "circumventing the GDPR."[11] The processing of biometric data, under the General Data Protection Regulation (GDPR), merits special protection. Given its sensitive nature, it entails high risks to the rights of individuals. Consequently, this precautionary measure is a decision based on exceptional circumstances to ensure immediate cessation of processing of personal data, preventing its possible transfer to third parties.[12]

INDIAN SENSITIVE DATA PROTECTION: AN UMBRELLA MADE OF TISSUE PAPER

While the implications of Spain's decision reverberate globally, they hold particular significance for countries like India, where discussions on data privacy and consent are increasingly central. As India charts its course in the digital age, navigating the complexities of regulatory frameworks and technological advancements becomes paramount. Worldcoin is accessible within India, where users have the opportunity to purchase[13] Worldcoin (WLD) via numerous cryptocurrency exchanges such as Binance and WazirX,[14] both of which provide trading pairs for Worldcoin. Furthermore, individuals residing in India can utilize the Worldcoin platform and obtain their World ID by utilizing an Orb, the device utilized by Worldcoin for eyeball-scanning verification. Despite certain temporary restrictions on Orb-verification services in India, it has not been banned yet.

[10]'The Agency Orders a Precautionary Measure Which Prevents Worldcoin from Continuing to Process Personal Data in Spain' (*AEPD*, 6 March 2024) <https://www.aepd.es/en/press-and-communication/press-releases/agency-orders-precautionary-measure-which-prevents-Worldcoin-from-continuing-toprocess-personal-data-in-spain#:~:text=The%20Spanish%20Data%20Protection%20Agency,block%20the%20data%20already%20collected.> accessed 9 May 2024.

[11]'Worldcoin and the AEPD in Spain' (*For every human*, 8 March 2024) <https://worldcoin.org/blog/worldcoin/worldcoin-aepd-spain> accessed 9 May 2024.

[12]Press A, 'Spain Puts Temporary Ban on Worldcoin Scans over Privacy Concerns' (*euronews*, 8 March 2024) <https://www.euronews.com/next/2024/03/08/spain-puts-temporary-ban-on-sam-altmans-worldcoin-eyeball-scans-over-privacy-concerns> accessed 9 May 2024.

[13](*Bitget*) <https://www.bitget.com/> accessed 9 May 2024.

[14]'Trading Platform: Wazirx' (*Buy Bitcoin, Cryptocurrency at India's Largest Exchange*) <https://wazirx.com/exchange/WLD-INR> accessed 9 May 2024.

A. Disappearing Distinguishing Factors on Sensitive Data in India

In Article 4, the GDPR meticulously delineates between various categories of personal data, a classification essential for assigning appropriate levels of security measures.[15] This categorization stratifies general personal data as the least sensitive, positioned at the bottom rung of the ladder, while elevating sensitive personal data to a higher tier, thereby demanding enhanced safeguards. Consequently, sensitive personal data becomes more arduous to obtain, underscoring the heightened level of protection it necessitates.[16]

This becomes particularly concerning for the data of minors or individuals in inherently data-sensitive sectors like the Armed Forces, as they are not afforded differential treatment. When juxtaposed with services that commodify biometrics and seek to normalize their usage, this scenario exacerbates risks. Hence, the imperative for categorizing data based on its sensitivity and implementing varied security measures becomes paramount to ensure privacy and mitigating potential harm.

B. Expected Changes with the Current Data Protection Regime,2023

Until replaced by the Digital Personal Data Protection Act, 2023; the Information Technology Act of 2000, specifically Section 43A,[17] addressed corporate liability in the handling of sensitive personal data or information, including biometric information. It mandated the implementation of reasonable security practices and procedures, such as the international standard IS/ISO/IEC 27001 or Government-approved codes of best practices for data protection, to safeguard biometric information and other sensitive data.[18]

[15]'Personal Data' (*General Data Protection Regulation (GDPR)*, 22 October 2021) <https://gdpr-info.eu/issues/personal-data/#:~:text=These%20data%20include%20genetic%2C%20biometric,convictions%20or%20trade%20union%20membership.> accessed 9 May 2024.

[16]European Union, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) OJ L119/1 (GDPR), art 4.

[17]Indian Information Technology Act 2000, s 43A.

[18] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, s 8(2)

RIGHT TO BE FORGOTTEN CONFLICTING WITH TRANS-BORDER DATA TRADE

Cryptocurrencies always have garnered acclaim for their capacity for expedited, secure, and cost-effective cross-border transactions, in contrast to conventional methods of international money transfers. By facilitating peer-to-peer transactions, circumventing intermediaries, and diminishing transaction expenses, cryptocurrencies offer a better experience.[19]

While individuals do have the right to have such data deleted, Worldcoin may however, under a contract, transfer sensitive personal information to any other corporate body or a person in India or located in any other country, which ensures the same level of data protection that is adhered to by the body corporate as provided for under the SPDI Rules.

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 ("The SPDI Rules") mandates collection for lawful purposes along with due consent.[20] The corporate body is obligated not to retain such data for longer than necessary;[21] however, in such a case, the duration of the 'necessity of such information' is indefinite as it is being used for authentication. The problem, makes itself apparent further when it comes to the cross-border transfer of such data. According to Section 7 of the Rules, such sensitive personal data or information including biometric information may be transferred to another entity provided that such transfer is necessary and the corporate entity is ensuring the same level of data protection that is adhered to by the body corporate.

Such laws depend on the good conscience of the countries where such data is being transferred. Once the data moves past India's jurisdiction, the clients are at the third party's mercy to ensure ethical handling of data with almost no recourse in the event of misuse. Challenges for transfer within India are equally threatening, once personal data becomes readily accessible in the Indian market, it poses significant risks. In the lack for a framework for cross-border sensitive information transfer, SPDI rules become unenforceable. While the Rules mention international Standard IS/ISO/IEC 27001 on "Information

[19]George AS, George ASH and Baskar T, 'Worldcoin: A Decentralized Currency for a Unified GlobalEconomy' (2023) 2 Partners Universal International Research Journal (PUIRJ)

[20] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, s 5(2)

[21] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, s 5(2)(b)

Technology – Security Techniques - Information Security Management System - Requirements" as a standard practice. The authors believes that where biometric information is coupled with financial information, the industry standard needs to be fortified with suitable solutions.

Undermining Degree of Risk Associated with Sensitive Information Breach

Merging individual identifiers obtained through biometrics with profiling methodologies can encroach upon the right to information self-determination. Profiling often entails the repurposing and reprocessing of information for objectives beyond their original scope. A "function creep" arises when technology is utilized for purposes diverging from its initial intent. Function creep may occur gradually over time, or controllers may harbour clandestine motives from the outset.[22]In societies grappling with systemic challenges related to race, religion, heteronormativity and caste, this can exacerbate issues of discrimination.

The dangers associated with the gathering and utilization of biometric information were starkly underscored by the Taliban's takeover of Afghanistan in 2022. During this tumultuous period, anti-government forces gained control and inherited a sophisticated biometric identification system originally developed by the U.S. military.[23] Known as the Handheld Interagency Identity Detection Equipment (HIIDES) system, it was initially devised to enable U.S. forces to swiftly identify individuals in the field and differentiate between allies and adversaries. However, the transfer of this system to the Taliban posed grave risks, as it could potentially expose the identities of individuals who had collaborated with American forces, placing them at risk of retaliation.[24] What was intended as an unambiguous identification tool, new became weaponized for purposes of vengeance, punishment, and exclusion.[25]

[22]Article 29 Data Protection Working Party, 'Guidelines on consent under Regulation 2016/679', WP259 rev.01, European Commission [2018] Available at: < https://ec.europa.eu/newsroom/article29/redirection/document/51030> [Accessed 3 May 2024].
[23]Faddis KN, Howard JJ and Stracener JT, 'Enhancing the Usability of Human Machine Interface on the Handheld Interagency Identification Detection Equipment (HIIDE)' [2011] 2011 21st International Conference on Systems Engineering.
[24](*Refile-feature-a year on, Afghans hide out fearing death by data | Reuters*) <https://www.reuters.com/article/idUSL8N2YT1H0/> accessed 9 May 2024
[25]Kerry CF and Wheeler T, 'The Enduring Risks Posed by Biometric Identification Systems' (*Brookings*, 9 February 2022) <https://www.brookings.edu/articles/the-enduring-risks-posed-by-biometric-identification-systems/> accessed 9 May 2024

Data that isn't acquired or handled in an ethical manner is more likely to find its way onto the Dark Web for sale. Privacy Affairs[26] conducted an investigation into the evolution of the Dark Web market since 2020 and observed a notable surge in personal and biometric data trading volume.[27]

While Worldcoins's policy may restrict data transfers at present, these policies are also subject to change. Fears fortify further when the company makes claims of limited responsibility for how the data is collected. During its launch, it identified 18 sites in Delhi, Noida, and Bangalore, where Orb operators conduct eye scans of individuals. It claimed that while operators undergo basic training and were 'encouraged' to adhere to a stringent Code of Conduct prioritizing legal compliance and public safety, they are not employees of Worldcoin. Last year December, Worldcoin paused iris scanning operations in India; however, the data procured in the past is still in the custody of Worldcoin.

Expectations from the Rules Replacing the SPDI Rules

The much-anticipated transition[28] from the Special Personal Data Protection Rules (SPDI Rules) to the DPDP Act, may not change much to the current situation. The Act's failure to clearly distinguish between layers of sensitive data[29] becomes a significant concern, which, at best, will maintain the dangerous status quo and, at worst, will worsen existing concerns. Without a nuanced understanding of the varying degrees of data sensitivity, the effectiveness of the transition remains in question, potentially leaving data protection measures inadequate or ambiguous.

[26]'Dark Web Price Index 2021 - Dark Web Prices of Personal Data' (*Privacy Affairs*, 10 June 2023) <https://www.privacyaffairs.com/dark-web-price-index-2021/> accessed 9 May 2024

[27]Pivcevic K, 'Biometric Selfies and Forged Passports: Identities for Sale on the Dark Web: Biometric Update' (*Biometric Update | Biometrics News, Companies and Explainers*, 18 April 2022) <https://www.biometricupdate.com/202106/biometric-selfies-and-forged-passports-identities-for-sale-on-the-dark-web> accessed 9 May 2024

[28]'India's Digital Transformation: A Deep Dive into Data Protection Act - ET Telecom' (*ETTelecom.com*, 17 August 2023) <https://telecom.economictimes.indiatimes.com/blog/indias-digital-transformation-a-deep-dive-into-data-protection-act/102786525> accessed 9 May 2024

[29]'Digital Personal Data Protection Act, 2023 – Key Highlights' (*azb*, 11 September 2023) <https://www.azbpartners.com/bank/digital-personal-data-protection-act-2023-key-highlights/> accessed 9 May 2024

CLIENT CONSENT MANAGEMENT, DATA TRADE AND FUTURE IMPLICATIONS OF SILENCE ON THE SUBJECT

A. Client Consent Management

While the temporary ban in Spain was what got the ball rolling, they weren't the first to take action on this. In August 2023, Kenya banned the operations of Worldcoin within the country as soon as it encountered the disruptive outcome of the reward system the company has been creating around data trade.[30]When the iris scans were functional in India, the company offered a sum of WLD coins to people who would participate in the iris scans,[31] which added a concerning aspect of "reward" associated with giving away (or selling; as explained before) of such data. The current landscape in India highlights a significant gap in data literacy among the general populace, leaving individuals ill-equipped to make informed decisions regarding the sharing of their sensitive information with data giants. The limited penetration of cryptocurrency into the mainstream populace has been a saving grace thus far. Whether it was due to the limited clientele of cryptocurrency in India or the fact that crypto transactions are yet to be as regular as UPI payments are. However, Worldcoin's mission to foster accessibility rather than exclusivity imposes a significant responsibility on the company to establish institutional structures capable of accommodating the diverse spectrum of individuals potentially involved in the project.

B. Minor Consent

Towards the end of March 2024, the company faced another ban from Portugal after it allegedly scanned the irises of minors, which is explicitly against the company's policy.[32] This raises multiple questions, firstly about the lack of systems in big-tech companies to ensure that their policies with regard to data security are followed on a grassroots level, and secondly the

[30]Nkonge A, 'Worldcoin Suspended in Kenya as Thousands Queue for Free Money' (*BBC News*, 3 August 2023) <https://www.bbc.com/news/world-africa-66383325> accessed 9 May 2024
[31]Venugopal S, 'Worldcoin: What Is Sam Altman's Biometric Project, and How Does It Work in India?' (*The Hindu*, 29 July 2023) <https://www.thehindu.com/sci-tech/technology/worldcoin-what-is-sam-altman-biometric-project-how-does-it-work-in-india/article67134353.ece> accessed 9 May 2024
[32]'Portugal: CNPD Temporarily Bans Worldcoin from Collecting Biometric Data for 90 Days' (*DataGuidance*, 27 March 2024) <https://www.dataguidance.com/news/portugal-cnpd-temporarily-bans-worldcoin-collecting> accessed 9 May 2024

understanding **of 'minor's consent'** and if a guardian's consent is even sufficient (as seen in most other cases) when it comes to sensitive personal data on the web.

The initial question revolves around the necessity of such discourse when minors are explicitly prohibited from participating in the project. Despite Worldcoin's approach in crafting policies aimed at securing minor consent, two significant barriers exist against their effectiveness. Firstly, a glaring absence of regulations specifically addressing sensitive data pertaining to minors in many countries, including India, poses a formidable challenge. States lack the obligation to penalize individuals who flout company policies for personal gain, thereby diminishing the risk-to-reward ratio associated with clandestine iris scans. Secondly, the company's handling of the situation thus far underscores a fundamental issue: individuals involved in ground-level data collection have minimal stakes in compliance, as they are not directly affiliated with the company. They lack the accountability structure necessary for policy enforcement, exacerbating the challenge of ensuring adherence to established protocols.

Under Section 9 of the DPDP Act, such data could be given by the consent of the data principal, who would be the parent/ guardian of the child in the present situation, the SPDI rules omit the discussion around the same, creating leeway for such interpretation around biometrics as well.[33]This moves us to a dystopian reality where the trade of biometric information of an individual who is a minor or infirm could bring monetary benefit to households. This becomes even more feasible for the event where there exists no method to cull out the age of the individual through any markers in the biometric data.One of the primary recommendations many academics put forth is the establishment of laws concerning minor consent. However, it's essential to recognize that minor consent regulation is more than just delineating who can consent to give their data. Acknowledging the vulnerability inherent in divulging such information and understanding the power dynamics at play between the individual empowered to grant consent on behalf of the minor and the minor is crucial.

Many players have raised questions on whether connecting the registration process to a centralised identity system, such as Aadhar in India, would be the answer to the question. Here the answer would have been yes, if it were not for Worldcoin's goal to made such

[33]Digital Personal Data Protection Act2023, s 9

authentication anonymous. This system attaches more identifiers to the biometric data, thereby making it more readily available for misuse.

C. Potential Role Models

The existence of a law to evince the state's obligation towards sensitive data privacy becomes foremost in this context. The Biometric Information Privacy Act 2008 (BIPA)may be the most stringent regulation of its kind in biometric protection.[34] Unlike other statutes, BIPA not only requires explicit consent for the gathering of biometric data, such as fingerprints or facial scans but also imposes strict guidelines for its protection. Furthermore, it prohibits the sale of biometric data and grants them the right to pursue legal action against companies for potential infringements. It has emerged as the benchmark for regulating biometric technologies, particularly facial recognition software. Advocacy groups, alongside individual consumers, have leveraged this law to litigate against numerous prominent companies.[35]

The intricacy deepens when the authority to consent to a minor's data is intertwined with a reward system, exemplified by giving away WLD Coins in this specific scenario. This intertwining calls to a futuristic-dystopia wherein the quantity of iris scans obtained from a single family directly correlates with the rewards reaped. Such a situation has the potential to compromise the integrity of decision-making processes, casting doubt on the ability to impartially assess whether such sensitive data should be disclosed in the first instance. The issue escalates further in countries where the local currency holds significantly lower value compared to the American Dollar.[36]

CONCLUSION: CRYPTO-GIVEAWAYS AND DATA TRADE

Addressing our research query, it is evident that Worldcoin lacks the necessary infrastructure to ensure adherence to its own policies within the prevailing regulatory framework governing sensitive personal data in India and numerous other nations. Consequently, it is ill-prepared to manage biometric data transfers effectively. Moreover, within the context of the ongoing Worldcoin operations, the ramifications of launching such ventures are intricately intertwined

[34]Biometric Information Privacy Act Illinois 2008
[35]Metz R, 'Here's Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois | CNN Business' (*CNN*, 20 September 2022) <https://edition.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html> accessed 9 May 2024
[36]Herrera LC and others, 'Worldcoin Is Surging in Argentina Thanks to 288% Inflation' (*Rest of World*, 1 May 2024) <https://restofworld.org/2024/worldcoin-argentina/> accessed 9 May 2024

with the social and economic fabric of the respective country. The effectiveness and implications of these "crypto-giveaways" could have been more thoroughly evaluated by considering the unique cultural contexts of each nation involved. Although they may not openly acknowledge this deficiency, it falls upon the respective states permitting such transactions to comprehend the potential repercussions of subjecting their citizens to this experimental scenario without adequate safeguards.

While a user may not directly profit from their personal data usage, it holds significant value for others. In 2019 alone, Facebook amassed a staggering $29.95 billion in net U.S. ad revenue, derived from approximately 231 million North American users.[37] Tech giants like Google and Amazon likely generated comparable, if not greater, revenue from one's data, primarily through digital advertising and retail endeavours. The extent of our control and compensation for such data depends on the legal framework of a given region. While India has acknowledged the necessity of compensation in the event of a data breach,[38] discussions concerning the user's right to part of the revenue generated through their data or remuneration for the data they give out have been reignited by ventures like Worldcoin.

Throughout this research paper, the author has proposed several recommendations. Firstly, there is a call for the reclassification of personal data into two distinct categories: general personal data and sensitive personal data. This would enable explicit regulation of security measures tailored to each category. Additionally, the delineation of Data Principles based on their vulnerability to potential data breaches. This would involve establishing separate thresholds for information processing, particularly for minors and individuals engaged in high-security professions. While the author believes that trading one's information is their choice, such choices must be well-informed to avoid data trade from becoming sucked in a quagmire of politics and vote bank. This lack of awareness underscores the urgent need for discussions surrounding the importance of consent managers at the grassroots level and comprehensive training on how to engage with the South Asian audience effectively. Despite the evident necessity, the discourse on the compulsion of having a data consent manager remains scarce

[37]Silver C, 'Council Post: Personal Data: Privacy vs. Compensation' (*Forbes*, 15 September 2020) <https://www.forbes.com/sites/forbestechcouncil/2020/09/16/personal-data-privacy-vs-compensation/?sh=71c8f8172aa2> accessed 9 May 2024
[38]Digital Personal Data Protection Act 2023, s 33(1)

within India, highlighting a critical area where attention and action are warranted to empower individuals in safeguarding their personal data privacy rights.

IMMUTABLE IDENTITIES: A COMPARATIVE STUDY OF INSURANCE COVERAGE OF BIOMETRIC PRIVACY CLAIMS IN THE UNITED STATES AND INDIA

—Sarthak Dash Bhattamishra[*]

ABSTRACT

As biometric data increasingly becomes essential for identity verification and access control, its unchangeable nature presents distinct legal and insurance challenges. This study explores the regulatory environments in the U.S. and India, emphasizing the need for clear policies and legal guidance, as illustrated by cases such as Krishna Schaumburg. The study highlights the potential benefits of EPL and D&O insurance policies in covering biometric data privacy claims, while also noting their limitations due to exclusions and ambiguities. The research advocates for a proactive approach in evaluating insurance coverage related to biometric data privacy, stressing the importance of strategic risk assessment and policy review. This study notes that India's IT Act and DPDP Act provide a foundational framework for data protection – however, their standards fall short of being comprehensive. The study calls for legislative reforms and advancements within the insurance industry to better align with international standards. By adopting best practices from the U.S., India can enhance its legal protections and better safeguard privacy rights, thereby strengthening defenses against the risks associated with digital identity theft and misuse.

Keywords: *Biometric Data; Privacy Law; Insurance Coverage; Regulatory Framework; EPL Policies; D&O Insurance; DPDP Act; Risk Assessment; Data Protection; Legal Disputes*

[*] The author is a Consultant at Grant Thornton Bharat.

I. INTRODUCTION

Our fingerprints don't fade from thedr(l)iveswe touch.

-Judy Blume

In a world where identity is increasingly defined by data, the permanence of biometric information makes it both a powerful tool and a significant vulnerability. Biometric data—whether it's a fingerprint, iris scan, or facial recognition profile—represents more than just a key to unlocking our devices or accessing secure locations. It embodies our unique identities, forever imprinted in the systems that safeguard our most sensitive information.

As the use of biometric technology becomes increasingly commonplace, its permanence becomes both a strength and a vulnerability. Unlike passwords or PINs, which can be changed if compromised, biometric data is inherently immutable.[1] This unchangeable nature makes it an ideal tool for security, yet it also exposes individuals and organizations to unprecedented risks. A single breach can have consequences, as these identifiers cannot be altered once they are out in the world.

This duality of biometric data—its power to protect and its potential to harm—necessitates a robust regulatory framework to manage its use. Countries around the world are grappling with how to balance the benefits of biometric technology with the need to protect individual privacy.[2]

In the digital age, biometric information has emerged as a unique and powerful form of personal data. It encompasses distinct biological and physical attributes such as retina and iris scans, fingerprints, voice patterns, facial recognition, and hand geometry. The use of biometric data[3] has become as commonplace as using a username and password for authentication and security.

[1]Sterling Miller, 'The basics, usage, and privacy concerns of biometric data' (Thomson Reuters, 20 July 2022) https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data accessed 17 August 2024

[2]Michael Odden, 'Biometric Crisis: Legal Challenges to Biometric Identification Initiatives' (2022) 39(2) Wisconsin International Law Journal 365-390 https://wilj.law.wisc.edu/wp-content/uploads/sites/1270/2022/09/39.2_365-390_Odden.pdf accessed 17 August 2024

[3] The GDPR's definition of biometric data is recognised globally due to its role as a comprehensive data protection benchmark. It influences global standards, especially for international data transfers, by being technologically neutral and adaptable to new technologies. The GDPR's risk-based approach applies stricter rules to sensitive biometric data, shaping global industry practices by encouraging thorough risk management.

Organizations worldwide are increasingly adopting biometric identifiers for a myriad of applications, from facial recognition on social media sites[4] to health and fitness monitoring[5] through wearable devices.[6] Biometric technology is also being utilized for customer verification in the retail and banking sectors[7], improving organizational security, employee timekeeping, and access to company-supplied workplace equipment.[8] Furthermore, certain businesses provide mobile applications that allow customers to virtually "try on" products using biometric data.[9]

However, the unchangeable nature of biometric data raises unique policy and security issues compared to traditional security information like login credentials and passwords. As a result, several countries have enacted both Central-Federal and State laws to regulate the collection, use, storage, and disclosure of biometric data. Companies that rely on biometric data face regulatory risks[10] and, under certain statutes, private or civil lawsuits[11].

Moreover, there has been a rising trend in the global legal landscape surrounding biometric data, particularly in the realm of insurance disputes and litigation over coverage for biometric

Under Article 4(14) of the GDPR, 'biometric data' refers to personal data derived from technical processing of an individual's physical, physiological, or behavioural traits that enable or confirm their unique identification, such as facial images or fingerprints.'Art. 4 GDPR – Definitions' (General Data Protection Regulation (GDPR)) https://gdpr-info.eu/art-4-gdpr/ accessed 17 August 2024

[4]Angela Petkovic, 'Companies Face Massive Biometric Information Privacy Act (BIPA) Allegations with Virtual Try-On Technology' (Journal of Technology and Intellectual Property, 6 November 2023) https://jtip.law.northwestern.edu/2023/11/06/companies-face-massive-biometric-information-privacy-act-bipa-allegations-with-virtual-try-on-technology/ accessed 17 August 2024

[5]'GoalMax', 'The Comprehensive Guide to Biometric Tracking in Sports and Fitness' (GoalMax Blogs, 6 January 2024) https://blogs.goalmax.net/the-comprehensive-guide-to-biometric-tracking-in-sports-and-fitness/ accessed 17 August 2024

[6]'Biometrics in Mobile Applications' (QASource Blog, 19 May 2021) https://blog.qasource.com/biometrics-in-mobile-applications accessed 17 August 2024

[7]'Deloitte Insights', 'Financial Institutions Face Massive Synthetic Identity Fraud Allegations' (Deloitte Insights, 27 July 2023) https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2023/financial-institutions-synthetic-identity-fraud.html accessed 17 August 2024

[8]'Biometrics Revolutionizing the Banking and Financial Sector' (Mantra Blog, 20 November 2019) https://blog.mantratec.com/biometric-in-banking-sector accessed 17 August 2024

[9]Zachary V. Zagger, 'Virtual 'Try On' Features: Do They Create Biometric Privacy Concerns for Retailers?' (Ogletree, 11 August 2022) https://ogletree.com/insights-resources/blog-posts/virtual-try-on-features-do-they-create-biometric-privacy-concerns-for-retailers/ accessed 17 August 2024

[10]The reference of 'regulatory risk' pertains to such risks that occur when a change in laws and regulations materially impact a security, business, sector, or market. A change in laws or regulations made by the government or a regulatory body can increase the costs of operating a business, reduce the attractiveness of an investment, or change the competitive landscape.

[11] A private lawsuit, also interchangeably referred to as a civil lawsuit in this research, is a non-criminal lawsuit brought by a private citizen, company, or entity of any name, against another party. It usually involves private property rights, including respecting rights stated under the Constitution or under Central/Federal or State law. Civil Case' (Legal Information Institute, Cornell Law School) https://www.law.cornell.edu/wex/civil_case accessed 17 August 2024

data privacy claims. In some instances, insurers agree to defend under a reservation of rights, implying they plan to provide a temporary defence while concurrently disputing coverage behind the scenes. Insurers may also outright deny coverage and initiate a declaratory judgment action seeking a court ruling that the biometric claim is not covered under the policy.

This study offers an in-depth comparison of the regulatory structures in India and the United States, with a special emphasis on the rising trend of insurance policies that address claims and costs related to biometric data privacy. It explores potential issues with coverage under these policies and suggests optimal practices for Indian organizations, especially in the context of the 2023 Digital Personal Data Protection Act ("DPDP Act"). These research questions aim to explore the intricacies of biometric data privacy laws and insurance coverage in the United States and India, the legal disputes arising from them, and endeavour to serve as the lessons India can learn from the U.S., the impact of India's DPDP Act, and the future trends in this domain:

1. **Comparative Regulatory Frameworks**: How do the regulatory frameworks for biometric data privacy in the United States and India differ? What are the key laws and regulations in each country, and how do they manage the collection, use, storage, and disclosure of biometric data?

2. **Insurance Coverage**: How do insurance policies in the United States address claims and costs related to biometric data privacy? What potential coverage issues arise under these policies, and how do they compare to those in India?

3. **Legal Disputes**: What are the common legal disputes involving biometric data privacy claims and insurance coverage in the United States? How have courts ruled in these cases, and what are the broader implications of these rulings?

4. **Lessons for India**: What insights can India gain from the United States' experience with biometric data privacy laws, regulations, and insurance coverage? How can these lessons inform India's approach to regulating biometric data and providing insurance coverage for related claims?

5. **Impact of the DPDP Act**: What is the anticipated impact of the Digital Personal Data Protection Act, 2023, on the handling of biometric data in India? How might this legislation influence the insurance industry and the coverage of biometric data privacy claims?

6. **Future Trends**: What emerging trends are shaping the global legal landscape surrounding biometric data, particularly in insurance disputes and litigation over coverage for biometric data privacy claims? How might these trends evolve, and what potential impact could they have on India?

In the US, biometric data privacy is regulated at the state level and, in certain cases, at the municipal level. Moreover, organizations with employees, customers, or business operations outside of the US must also adhere to any data protection or sector-specific laws governing the collection and use of biometric data, such as the General Data Protection Regulation.[12]

The following sections will delve deeper into these topics, providing a comprehensive overview of the current state of biometric data regulation and its implications for businesses in India and the US.

This research thoroughly examines the intricate landscape of biometric data privacy laws and insurance coverage in both (certain States of) the United States and India. With the increasing use of biometric data across various sectors, it is crucial for businesses and policymakers to grasp the associated regulatory risks and insurance challenges. The study seeks to address existing gaps in the literature by offering a comparative analysis of the regulatory frameworks in these two countries, an area that has seen limited exploration. Additionally, it delves into the emerging trend of insurance policies that cover biometric data privacy claims, a rapidly evolving domain that demands up-to-date research.

The findings of this research could have far-reaching implications, particularly for businesses in India in the wake of the DPDP Act. By drawing lessons from the U.S. model, Indian businesses can more effectively navigate the regulatory landscape and manage their insurance coverage. Furthermore, this research could provide valuable insights for policymakers in India as they continue to develop and refine biometric data privacy regulations, ensuring that these laws are robust, effective, and aligned with global best practices.

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

II. APPLICABLE STATE AND MUNICIPAL REGULATIONS IN THE US CONCERNING BIOMETRIC DATA

In the United States, several states, including Illinois, Texas, and Washington, have enacted laws specifically addressing the management of biometric data. These include:

- The Biometric Information Privacy Act ("BIPA") in Illinois – Enacted in 2008, BIPA was among the first laws to specifically safeguard biometric information. It mandates that companies must obtain explicit consent from both consumers and employees before collecting, storing, or using their biometric data. Additionally, BIPA grants individuals the right to file lawsuits for violations, which can result in substantial penalties for non-compliance. The legislation was introduced to mitigate identity theft risks and to promote public confidence in biometric-based transactions. Over time, amendments have been made to BIPA to limit the instances that qualify for claims under a private right of action[13];
- The Capture or Use of Biometric Identifier Act ("Biometric Identifier Act") in Texas – the Texas Biometric Identifier Act, which predates BIPA by seven years, was the first state law to regulate the collection and use of biometric data. This legislation prohibits the commercial collection of biometric identifiers from individuals without their explicit consent. Enforcement of the Act is exclusively the responsibility of the Texas Attorney General. Enacted to safeguard residents, the law aims to prevent unauthorized organizations or individuals from entering biometric information into databases without proper consent.[14]; and,
- The law concerning biometric identifiers ("Revised Code of Washington") in Washington State – the Revised Code of Washington, enacted in 2017, governs the collection, disclosure, and retention of biometric identifiers. Under this law, businesses are required to inform individuals and obtain their consent before collecting biometric data for commercial use. The legislation was introduced in response to growing concerns in the Washington State legislature about the increasing frequency with which citizens were being asked to

[13] Biometric Information Privacy Act, 740 ILCS 14/5 (2023).' Available at: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57 (last visited Aug. 17, 2024).
[14] 'Texas Business & Commerce Code, § 503.001 (2024).' Available at: https://statutes.capitol.texas.gov/docs/bc/htm/bc.503.htm (last visited Aug. 17, 2024).

provide sensitive biometric information for purposes such as commerce, security, and convenience.[15]

In addition to these specific laws, many states have implemented regulations that address certain aspects of biometric data. Some states, for instance, have:

Enacted laws that regulate biometric data in the context of employment laws[16], identity theft protection laws[17], and laws governing the collection of biometric data by public schools[18];

- Included unique biometric data of an individual in the definition of personal information in their general data breach notification statutes[19]; and passed comprehensive privacy laws that incorporate biometric information in the definition of personal information. This

[15]'Revised Code of Washington, §§ 19.375.010 to 19.375.040 (2024).' Available at: https://app.leg.wa.gov/RCW/default.aspx?cite=19.375&full=true (last visited Aug. 17, 2024).

[16] Such states that have enacted laws that regulate the use of biometric data in the context of employment include:

- Illinois, via the BIPA;
- Texas, via the Biometric Identifier Act;
- Washington, via the Revised Code of Washington;
- California, via the California Consumer Privacy Act ('California Civil Code, Division 3, Part 4, Title 1.81.5 (2024).' Available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (last visited Aug. 17, 2024).) read with the California Labor Code ('California Labor Code (2024)' Availableat: https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=LAB&tocTitle=+Labor+Code+-+LAB (last visited Aug. 17, 2024);
- New York, via the New York Labor Law ('New York Labor Law § 201-A (2024).' Available at: https://www.nysenate.gov/legislation/laws/LAB/201-A (last visited Aug. 17, 2024); and,
- Oregon, via the Oregon Consumer Identity Theft Protection Act ('Oregon Revised Statutes, Title 50, Chapter 646A, Section 646A.602 (2024).' Available at: https://casetext.com/statute/oregon-revised-statutes/title-50-trade-regulations-and-practices/chapter-646a-trade-regulation/identity-theft-prevention/section-646a602-definitions-for-ors-646a600-to-646a628 (last visited Aug. 17, 2024).

[17]States like Illinois, Texas, and Washington have passed legislation regulating private entities' collection and processing of biometric information. A comparison between the data privacy and protection legislation of the three States can be found at: 'Bloomberg Law, Biometric Data Privacy Laws (2024).' Available at: https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/#state (last visited Aug. 17, 2024)

[18]BIPA of Illinois, and Biometric Identifier Act of Texas.

[19]The States of Illinois, Iowa, Nebraska, North Carolina, Wisconsin, and Wyoming include unique biometric data, such as a fingerprint, retina or iris image, or other unique representation of biometric data when used with a first name/initial and last name in their data breach notification laws. 'National Law Review, State Data Breach Notification Laws – Overview of Requirements for Responding to a Data Breach (2024).' Available at: https://natlawreview.com/article/state-data-breach-notification-laws-overview-requirements-responding-to-data-1 (last visited Aug. 17, 2024)

includes states like California[20], Colorado[21], Connecticut[22], Indiana[23], Iowa[24], Montana[25], Tennessee[26], Utah[27], and Virginia[28].

Several cities in the US, including Baltimore[29], New York City[30], and Portland (Oregon)[31], have also passed ordinances that govern biometric data. The common thread amongst such city-council ordinances is the common mandate for certain commercial establishments to disclose their practices of collecting and using biometric data and prohibit the sale of such data. It is trite to mention that companies that utilize biometric data are subject to regulatory risks and potential private lawsuits. While the statutory requirements and restrictions concerning biometric data vary by jurisdiction, common themes include:

- The requirement of some form of notice about the collection and use of biometric information;

[20]Via the California Consumer Privacy Act

[21] Via the Corado Revised Statutes, part of the Colorado Consumer Protection Act. 'Colorado Revised Statutes, Title 6, Article 1, Part 7, Section 6-1-716 (2024).' Available at: https://law.justia.com/codes/colorado/2022/title-6/article-1/part-7/section-6-1-716/ (last visited Aug. 17, 2024)

[22] Via the Connecticut General Statutes, which is a part of the Connecticut Consumer Data Privacy and Online Monitoring Act. 'Connecticut General Statutes, Title 42, Chapter 743jj, Section 42-515 (2024).' Available at: https://law.justia.com/codes/connecticut/2022/title-42/chapter-743jj/section-42-515/ (last visited Aug. 17, 2024)

[23]Via the Indiana Code § 24-15-2-4, which will be effective from January 01, 2026, and which is a part of the Indiana Consumer Data Protection Act. 'Indiana Code, Title 24, Article 15, Chapter 2, Section 24-15-2-4 (2024).' Available at: https://casetext.com/statute/indiana-code/title-24-trade-regulation/article-15-consumer-data-protection/chapter-2-definitions/section-24-15-2-4-effective-112026-biometric-data (last visited Aug. 17, 2024)

[24] Via the Iowa Code Ann. § 715D.1(4), (26), which will be effective from January 01, 2025, and which is a part of the Iowa Consumer Data Protection Act. 'Code of Iowa, Title XVI, Chapter 715D, Section 715D.1 (2024).' Available at: https://casetext.com/statute/code-of-iowa/title-xvi-criminal-law-and-procedure/chapter-715d-consumer-data-protections/section-715d1-effective-112025-multiple-versions-definitions (last visited Aug. 17, 2024)

[25] Via the Montana Code Ann. § 30-14-2802(3), which will be effective from October 01, 2024, and which is a part of the Montana Consumer Data Privacy Act. 'Montana Code Annotated, Title 30, Chapter 14, Part 28, Section 20 (2024).' Available at: https://www.leg.mt.gov/bills/mca/title_0300/chapter_0140/part_0280/section_0020/0300-0140-0280-0020.html (last visited Aug. 17, 2024)

[26]Via the Tennessee Public Act Ch. 408 § 2, which will be effective from July 1, 2025, and which is a part of the Tennessee Information Protection Act. 'Tennessee House Bill 1181, 113th General Assembly (2024).' Available at: https://legiscan.com/TN/bill/HB1181/2023 (last visited Aug. 17, 2024)

[27]Via the Utah Code § 13-61-101(6)(b), which is a part of the Utah Consumer Privacy Act (Link)

[28] Via the Virginia Code Ann. § 59.1-575, which is a part of the Virginia Consumer Data Protection Act (Link)

[29]Baltimore Council Bill 21-0001. 'Utah Code, Title 13, Chapter 61 (2024).' Available at: https://le.utah.gov/xcode/Title13/Chapter61/C13-61_2022050420231231.pdf (last visited Aug. 17, 2024).

[30]New York City Department of Consumer and Worker Protection read with the New York City Administrative Code § 22-1201 (Biometric Identifier Information law). 'New York City Department of Consumer and Worker Protection, Rule regarding Biometric Data Collection (2024) and New York City Administrative Code (2024).' Available at: https://rules.cityofnewyork.us/wp-content/uploads/2021/07/NOA_DCWP-Rule-re-Biometric-Data-Collection.pdf and https://codelibrary.amlegal.com/codes/newyorkcity/latest/NYCadmin/0-0-0-131254 (last visited Aug. 17, 2024).

[31]'City of Portland, Privacy Protection Policies (2024).' Available at: https://www.portland.gov/bps/smart-city-pdx/about-privacy-program/privacy-protection-policies (last visited Aug. 17, 2024)

- The requirement of explicit consent, sometimes in writing, from individuals to use their biometric data;
- Restrictions on the sale, lease, or other disclosure of biometric information to varying degrees; and,
- Standards for confidentiality, retention, and disposal of biometric data when it is no longer needed for the purpose of collection.

For instance, in terms of enforcement mechanisms, BIPA allows an 'aggrieved person' to file a lawsuit in state or federal court and recover:

- For each negligent violation, the greater of liquidated damages of $1,000 or actual damages;
- For each intentional violation, the greater of liquidated damages of $5,000 or actual damages;
- Reasonable attorneys' fees and costs; and,
- Injunctive or other appropriate relief.[32]

On the other hand, only the attorneys general of the States of Texas and Washington can initiate actions to enforce their statutes, i.e., the Biometric Identifier Act and the Revised Code of Washington, respectively.

III. COMPLEXITIES OF CYBER INSURANCE FOR BIOMETRIC DATA PRIVACY CLAIMS

Cyber insurance can offer crucial coverage for organizations facing potential or actual violations of biometric data privacy laws. However, comparing policies and choosing suitable cyber coverage is often complex due to the lack of standardization in policies and the intricate nature of data risks.[33] For instance, two policies may use the same terms, such as 'security

[32]Section 20, BIPA. 'Illinois Compiled Statutes, Chapter 740, Act 740 ILCS 14 (2024).' Available at: https://law.justia.com/codes/illinois/chapter-740/act-740-ilcs-14/ (last visited Aug. 17, 2024).

[33]The FTC recommends that businesses explore cyber insurance as a means to mitigate the financial impact of cyber-attacks. It suggests that companies carefully assess whether they need first-party, third-party, or a combination of both coverages. The FTC advises that a robust cyber insurance policy should cover key areas such as data breaches, including those involving third-party vendors, global cyber-attacks, and incidents categorized as terrorist acts. Additionally, the FTC encourages businesses to consider whether their insurance provider will offer defence in lawsuits or regulatory investigations, coverage beyond other existing insurance policies, and a 24/7 breach hotline. For first-party coverage, the FTC suggests that businesses ensure protection for their data and associated costs, including legal counsel, data recovery, customer notification, business interruption, crisis management, and forensic services. For third-party coverage, the FTC advises that companies should be protected against liability claims from third parties, such as payments to affected consumers, litigation costs, defamation, copyright or trademark infringement, and settlements.'Federal Trade Commission, Cybersecurity for Small

event', or 'regulatory investigation', but define those terms differently, leading to significant variations in the coverage provided.

Differences in coverage across policies can be substantial and may include variations in the triggering of notice requirements, the scope of coverage (including regulatory exposures), aggregate policy limits and sub-limits, self-insured retentions, and coverage periods (including retroactive coverage). Two policies may use the same terms but define them differently, leading to significant variations in coverage. For instance, the term 'security event' could be defined in one policy as a breach of network security that results in unauthorized access to or use of data, while another policy might define it as any act or attempt to gain unauthorized access to the system, regardless of whether data is accessed.[34]

Likewise, the scope of coverage can vary significantly across policies. Some policies might offer broad coverage that includes regulatory exposures, while others might have more limited coverage. For example, one policy might cover regulatory fines and penalties associated with a data breach, while another policy might exclude such costs.[35]

The complexities of cyber insurance for biometric data privacy have implications for businesses, presenting several challenges for policyholders. One major bottleneck is the difficulty in understanding policy terms due to the lack of standardization and the intricate nature of data risks. This can lead to misunderstandings about coverage and potential gaps in protection. Additionally, the considerable variations in coverage across different policies make it challenging for policyholders to compare options effectively, often resulting in the purchase of policies that do not adequately address their specific risks.[36]

Businesses: Cyber Insurance (2024).' Available at: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/cyber-insurance (last visited Aug. 17, 2024).

[34]'Cybersecurity Dive, How Cyber Insurance Coverage is Evolving (2024).' Available at: https://www.cybersecuritydive.com/news/cyber-insurance-coverage-evolution/721171/ (last visited Aug. 17, 2024).

[35]'Cyber Defense Group, Cyber Insurance Guide (2024).' Available at: https://www.cdg.io/blog/cyber-insurance-guide/ (last visited Aug. 17, 2024).

[36]'Miller Friel, Insurance Coverage for Biometric Data Privacy Claims (2024).' Available at: https://millerfriel.com/wp-content/uploads/2021/07/Insurance-Coverage-for-Biometric-Data-Privacy-Claims-w-031-3339.pdf (last visited Aug. 17, 2024).

Cyber policies should cover biometric data privacy claims unless there are any exclusions or limiting language. However, policyholders should thoroughly review their policies to ensure that biometric data privacy claims are not excluded in any way. For example:

- Cyber policies typically cover claims arising from 'privacy events' or 'privacy and security wrongful acts' which may include the unlawful or unauthorized disclosure of confidential or private data. This language should cover violations of biometric data privacy laws based on the unauthorized collection, storage, or other use of the data, including unauthorized transmission of that data to third parties.[37] However, organizations must carefully review this language to ensure coverage;
- Some cyber policies may define 'confidential' or 'private' data in a way that may exclude biometric data and limit coverage[38]; and,
- Some cyber policies limit or exclude coverage for claims arising under specific, enumerated statutes, such as biometric data privacy laws.[39]

IV. CYBER INSURANCE IN ADDRESSING BIOMETRIC DATA PRIVACY LAW VIOLATIONS

Cyber insurance can offer essential coverage for organizations dealing with potential or actual breaches of biometric data privacy laws. Although in the US, at the time of this research being undertaken, there are no published decisions regarding companies seeking coverage for violations of biometric data privacy laws under cyber policies. However, many policyholders without cyber insurance have managed to secure coverage for losses related to biometric data in recent years under traditional, non-cyber policies.[40]

[37]'Miller Friel, Insurance Coverage for Biometric Data Privacy Claims (2024).' Available at: https://millerfriel.com/wp-content/uploads/2021/07/Insurance-Coverage-for-Biometric-Data-Privacy-Claims-w-031-3339.pdf (last visited Aug. 17, 2024).

[38]'Bloomberg Law, Insurers Add Biometric Exclusions as Privacy Lawsuits Pile Up (2024).' Available at: https://news.bloomberglaw.com/insurance/insurers-add-biometric-exclusions-as-privacy-lawsuits-pile-up (last visited Aug. 17, 2024).

[39] For instance, as per Section 1798.140(o)(1)(E), the CCPA defines '*Biometric information'* as an individual's physiological, biological, or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

[40]'Biometric Update, Attorneys Explain Insurance Coverage for Biometric Privacy Lawsuits (2024).' Available at: https://www.biometricupdate.com/201711/attorneys-explain-insurance-coverage-for-biometric-privacy-lawsuits (last visited Aug. 17, 2024).

A. Commercial General Liability (CGL) Policies

CGL policies usually provide coverage for 'personal and advertising injury', in addition to coverage for bodily injury and property damage. Personal and advertising injury in CGL policies is typically defined as an injury resulting from the oral or written publication of material that infringes on a person's right to privacy. Some CGL policies contain exclusions, which insurers argue prevent coverage for biometric data privacy claims.[41]

B. Disputes Over "Publication"

In insurance policies, the term "publication" generally refers to the act of making information public or widely known. In the context of biometric data privacy claims, "publication" often pertains to the sharing or disclosure of biometric data. Disagreements over this term arise when there is a conflict between the insurer and the policyholder regarding whether the sharing or disclosure of biometric data qualifies as a "publication" under the policy's terms. This issue is critical because, if a biometric data privacy event is not deemed a "publication," it may not activate the personal and advertising injury coverage in the policy.[42]

These disputes frequently center on the specific wording and definitions within the policy.[43] For instance, some policies might define "publication" as the communication of information to the general public, while others may interpret it as the sharing of information with any third party. The lack of standardization in policy language can result in varying interpretations and disputes over coverage.

The consequences of these disputes for businesses can be significant. If an insurer's narrow interpretation of "publication" is upheld, a business might find itself without coverage for a biometric data privacy claim, even if it holds a CGL policy or a cyber insurance policy.[44] This could leave the business vulnerable to substantial financial and reputational risks. Conversely,

[41]'Nicolaides Fink Thorpe Michaelides Sullivan LLP, Biometric Privacy and Data Breach Insurance Recovery (2020).' Available at: https://www.nicolaidesllp.com/siteFiles/Insights/BIPADRI2020.pdf (last visited Aug. 17, 2024).
[42]*Ibid.*
[43]'Legal Dive, Biometric Privacy Settlements Spark Insurance Coverage Battles (2024).' Available at: https://www.legaldive.com/news/biometric-privacy-settlements-spark-insurance-coverage-battles-BIPA-Wilson-Elser-anderson-kill/708562/ (last visited Aug. 17, 2024)
[44]'Claims Journal, National News (2023).' Available at: https://www.claimsjournal.com/news/national/2023/08/15/318654.htm (last visited Aug. 17, 2024).

if a broader interpretation of "publication" is accepted, it could provide businesses with essential coverage for biometric data privacy claims, helping them manage financial risks and potentially enhancing their reputation by showing that they have appropriate insurance coverage.

Personal and advertising injury in CGL policies is typically defined as oral or written publication, in any manner, of material that violates a person's right to privacy. In the past, insurers often disputed coverage for BIPA lawsuits filed against the insured, arguing that the underlying lawsuits did not specifically allege 'publication' of material that violates a person's right to privacy. Hence, inadvertently, most courts in the US have denied coverage for cyber incidents under CGL policies. They have either determined that there was no "publication" of private material[45] or found that the "publication" by a third party, rather than the insured, was inadequate.[46]

In one of the landmark cases pertaining to 'publication', in West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc. ("Krishna Schaumburg"), the Supreme Court of Illinois specifically rejected this argument and ruled that CGL policies with this language cover BIPA claims. In Krishna Schaumburg, the insurer filed a declaratory judgment action seeking a determination that it did not owe its insured, a tanning salon, a duty to defend a class action lawsuit alleging BIPA violations arising from the disclosure of fingerprint information to a third-party vendor. The policies specifically defined "personal injury" and "advertising injury" as injury arising out of oral or written publication of material that violates a person's right to privacy.[47]

[45] For instance, in Recall Total Information Management, Inc. v. Federal Ins. Co., the Connecticut Supreme Court determined that Federal Insurance Company was not obligated to cover losses from an incident where computer tapes with private information fell out of the back of a van, were picked up by an unidentified individual, and were never recovered. The court concluded that there was no "publication" that would activate the policy coverage, as there was no evidence that anyone had accessed the confidential information on the tapes. 'Recall Total Information Management, Inc. v Federal Insurance Co, 83 A.3d 664 (2014) and 115 A.3d 458 (2015).' Available at: https://casetext.com/case/recall-total-info-mgmt-inc-v-fed-ins-co-1 (last visited Aug. 17, 2024).

[46]Even when private information is "published," courts have found that CGL policies only cover publication by the policyholder, not by third parties like hackers. For example, in March 2014, the New York Supreme Court examined whether CGL coverage applied to the PlayStation Network data breach in the case of Zurich American Insurance Company v. Sony Corporation of America, et al. The court ruled that although there was a "publication" of confidential information, coverage did not extend because the publication was executed by a third party, not by Sony, the insured. Sony appealed, but the case was settled in 2015 before the appellate court could issue a ruling.'New York Appellate Division, First Department, 2015 NY Slip Op 09599.' Available at: https://law.justia.com/cases/new-york/appellate-division-first-department/2015/651982-11-14547-14546.html (last visited Aug. 17, 2024).

[47]'Illinois Supreme Court, 2021 IL 125978 (2021).' Available at: https://law.justia.com/cases/illinois/supreme-court/2021/125978.html (last visited Aug. 17, 2024).

The insurer argued that a personal and advertising injury did not exist because "publication" requires communication of information to the public at large, not a single third party. The court rejected that argument and held that:

- The disclosure of the customer's fingerprint to a single vendor in alleged violation of BIPA constituted a publication under the common understanding and dictionary definition of the term; and,
- The allegations in the class action complaint that the policyholder tanning salon shared biometric data with a third party constituted a covered claim for "personal and advertising injury" within the purview of the policies.

Krishna Schaumburg has addressed numerous complaints from insurers who argued similarly about the interpretation of "publication" to deny BIPA coverage. For instance, in State Automobile Mutual Insurance Company v. Tony's Finer Foods Enterprises, Inc.("Tony's Finer Foods"), the court granted the insurer's motion to withdraw certain previous arguments regarding "publication" following the Krishna Schaumburg ruling.[48]The takeaway from these catenae of judicial pronouncements is that organizations looking to use CGL coverage for claims related to biometric data privacy law violations need to carefully review their policy language concerning "publication" and be aware of potential arguments insurers might use to deny regulatory coverage, including but not limited to BIPA.

C. Exclusions Related to Employment Practices

CGL policies may contain personal and advertising injury exclusions claiming to bar coverage for personal and advertising injuries arising out of employment-related practices, policies, acts, or omissions. Several insurers have disputed coverage based on this language for costs to defend against employee lawsuits alleging biometric data privacy law violations. The insurers have presented several defences against providing coverage. The primary argument of the insurers has been that the underlying complaints do not qualify as a "personal injury" under the policy's definition. Additionally, they claim that coverage is barred by the Employment

[48]'State Automobile Mutual Insurance Company v. Tony's Finer Foods Enterprises, Inc., No. 1:2020cv06199, N.D. Ill. (2022).' Available at: https://casetext.com/case/state-auto-mut-ins-co-v-tonys-finer-foods-enters (last visited Aug. 17, 2024).

Practices Liability exclusion, the Recording and Distribution (or Violation of Statutes) exclusion, and the Access or Disclosure exclusion.[49]

Courts have split on whether the employment-related practices exclusion bars coverage for privacy claims. Returning to Tony's Finer Foods, the court held that the exclusion did not apply because "employment-related practices" only apply to adverse employment actions, such as changes in employment status or other negative treatment directed at employees, and to "not any and all claims about something that happens at work."[50] Similarly, in yet another case, the court rejected the plea of holding the exclusion because it was unclear whether the alleged violations shared "general similitude with … the matters specifically enumerated in the employment-related practices exclusion."[51]On similar lines, courts have also held that "employment-related practices exclusion did not apply"[52],and that "exclusion barred coverage for a claim brought by the insured's employee alleging BIPA violations arising out of a fingerprint-scanning timekeeping system."[53]

However, a subsequent appellate decision has provided further guidance, holding that the exclusion of employment-related practices does not bar coverage for BIPA claims and that exclusions did not apply because the handprint-scanning system was not "directed towards" any given worker.[54] The plain meaning of the exclusion suggests that it should only apply to, "a change in an employee's standing, or targeted mistreatment of a specific person — that is, conduct 'directed at that person.'"[55] By contrast, even if the fingerprint or handprint

[49]For instance, Citizens Insurance Company of America v. Northwest Pallet Services, LLC, where the Plaintiff argued that it had no duty to defend or indemnify the Defendant for claims connected to an underlying putative class action filed under the BIPA. 'Justia Dockets, Illinois Northern District Court, 1:2021cv02804 (2024).' Available at: https://dockets.justia.com/docket/illinois/ilndce/1:2021cv02804/403943 (last visited Aug. 17, 2024).

[50] Supra 48

[51]Citizens Insurance Company of America, and Hanover Insurance Company v. Thermoflex Waukegan, LLC. 'Insurance Coverage for Biometric Data Claims, US (2024).' Available at: https://d.docs.live.net/3a6529157aa2c20c/Documents/Sarthak Transfer/Work Dox/Writings/Insurance Coverage_Biometric Data Claims/US.docx (last visited Aug. 17, 2024).

[52]Society Insurance v. Cermak Produce No. 11, Inc. 'Society Insurance v. Cermak Produce No. 11, Inc., 21 CV 1510, United States District Court, Northern District of Illinois (2023).' Available at: https://casetext.com/case/socy-ins-v-cermak-produce-no-11-inc (last visited Aug. 17, 2024).

[53] American Family Mutual Insurance Company v. Caremel, Inc.& Others. 'American Family Mutual Insurance Co. v. Caremel, Inc., 20 C 637, United States District Court, Northern District of Illinois (2022).' Available at: https://casetext.com/case/am-family-mut-ins-co-v-caremel-inc (last visited Aug. 17, 2024).

[54]Thermoflex Waukegan, LLC v. Mitsui Sumitomo Insurance USA, Inc. 'Federal Appellate Courts, No. 23-1578 (7th Cir. 2024).' Available at: https://law.justia.com/cases/federal/appellate-courts/ca7/23-1578/23-1578-2024-05-17.html (last visited Aug. 17, 2024).

[55] Supra 48, Tony's Finer Foods

timekeeping systems at issue in so many privacy claims' coverage disputes are employment-related practices or policies, they apply to all employees generally and are not directed at specific individuals. A general policy mandating all hourly workers to use a hand scanner is an employment-specific practice, but it is not 'directed towards' any individual employee. The inclusion of phrases like 'directed towards that person' refer to actions specific to a particular employee.[56]

V. STATUTORY EXCLUSIONS IN COMMERCIAL GENERAL LIABILITY POLICIES

A. *Exclusions in CGL Policies*

CGL policies contain exclusions that prevent coverage for personal and advertising injury claims, that arise directly or indirectly from any action or omission that infringes or is alleged to infringe, that arise under statutes, ordinances, or regulations that restrict or limit the sending, transmitting, communicating, or distribution of material or information.[57] For instance, a company that sends promotional emails might be sued for spamming, and would be deemed to be in violation of the CAN-SPAM Act.[58] If the company's CGL policy has a statutory exclusion for violations of laws that restrict or limit the sending, transmitting, communicating, or distribution of material or information, the insurer could deny coverage for this claim.

When it comes to implications, statutory exclusions in CGL policies can restrict coverage for personal and advertising injury claims related to any action or omission that violates or is alleged to violate laws, statutes, ordinances, or regulations.[59] This limitation can leave businesses vulnerable to substantial financial liability in the event of a lawsuit. For example, on the legal front, a court's interpretation of such exclusions may affect subsequent cases, leading to uncertainty and potential inconsistency in how such exclusions are applied.[60]

[56]Supra 54

[57] For instance, the Telephone Consumer Protection Act of 1991 and the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. 'Federal Communications Commission, Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 (2024) and Federal Trade Commission, Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (2024).' Available at: https://www.fcc.gov/sites/default/files/tcpa-rules.pdf and https://www.ftc.gov/legal-library/browse/statutes/controlling-assault-non-solicited-pornography-marketing-act-2003-can-spam-act (last visited Aug. 17, 2024)

[58]'Federal Trade Commission, Protecting Personal Information: A Guide for Business (2024).' Available at: https://www.govinfo.gov/content/pkg/GOVPUB-FT-PURL-LPS104106/pdf/GOVPUB-FT-PURL-LPS104106.pdf (last visited Aug. 17, 2024).

[59]'Thompson Coe, Common Liability Exclusions: The Good, The Bad and The Ugly (2024).' Available at: https://www.thompsoncoe.com/resources/publications/common-liability-exclusions-the-good-the-bad-and-the-ugly/ (last visited Aug. 17, 2024).

[60] Case on point, Krishna Schaumburg

Returning to the case of Krishna Schaumburg, the insurer argued that the policies' "other than" language in the violation of statutes exclusion prevented coverage for the alleged BIPA disclosures. However, the court disagreed, stating that this exclusion only applies to statutes that govern specific methods of communication, such as emails, faxes, and phone calls, and does not apply to statutes that, "restrict the sending or sharing of certain information," such as BIPA.[61]

B. *Impact of Krishna Schaumburg Ruling*

The ruling of Krishna Schaumburg on the statutory exclusion language for privacy claims coverage has influenced other cases making similar arguments. However, courts have been divided on whether a slightly different version of this exclusion, called "distribution of material in violation of statutes," prevents coverage for "personal and advertising injury" arising directly or indirectly out of any action or omission that infringes or is alleged to infringe laws, statutes, ordinances, or regulations that address, prohibit, or limit the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating, or distribution of material or information.[62]

C. *Disputes Over "Access to or Disclosure of Confidential or Personal Information" Exclusion*

Lawsuits filed by insurers disputing biometric data-related coverage concern policy language excluding personal and advertising injury coverage arising out of access to or disclosure of any person's or organization's confidential or personal information, including:

- Patents, trade secrets, processing methods, and customer lists.
- Financial and credit card information.
- Health information.
- Any other type of non-public information.[63]

[61] Supra48

[62]Massachusetts Bay Insurance Company, The Hanover American Insurance Company, and The Hanover Insurance Company v. Impact Fulfillment Services, LLC, and IFS Holding, LLC. 'Massachusetts Bay Insurance Co. v. Impact Fulfillment Services, 1:20CV926, United States District Court, Northern District of Illinois (2023).' Available at: https://casetext.com/case/mass-bay-ins-co-v-impact-fulfillment-servs (last visited Aug. 17, 2024).

[63]For instance, see Citizens Insurance Company of America v. Mullins Food Products, Inc., and Ricardo Galan.'Citizens Insurance Company of America v. Mullins Food Products, Inc., 22-cv-1334, United States District Court, Northern District of Illinois (2024).' Available at: https://casetext.com/case/citizens-ins-co-of-am-v-mullins-food-prods (last visited Aug. 17, 2024).

Insurers have argued that biometric data falls within confidential or personal information and the exclusion bars coverage for claims alleging biometric data disclosures.[64] Courts have split on whether this exclusion bars coverage for biometric claims. Hence, for instance, in a hypothetical where a healthcare provider is sued for a data breach that exposed patients' health information. If the provider's insurance policy excludes coverage for personal and advertising injury arising out of access to or disclosure of any person's or organization's confidential or personal information, the insurer could argue that this exclusion bars coverage for the data breach claim. This exclusion could lead to disputes about whether biometric data is considered confidential or personal information.[65] If insurers assert that this exclusion denies coverage for claims involving the disclosure of biometric data, businesses could be at considerable financial risk if they are sued for such disclosures.[66]

D. *Data Breach Liability Exclusion*

A frequently litigated exclusion states that the policy does not cover:

- Loss arising out of disclosure of or access to private or confidential information belonging to any person or organization; or;
- Any loss, cost, expense, or 'damages' arising out of damage to, corruption of, loss of use or function of, or inability to access, change, or manipulate "data records."[67]

To cite an example, a retail company suffers a cyber-attack that results in the theft of customers' credit card information. The company's insurance policy has a data breach liability exclusion that states the policy does not cover loss arising out of disclosure of or access to private or confidential information. In this case, the insurer might deny coverage for the cyber-attack claim based on this exclusion.

[64]Supra 48, Tony's Finer Foods
[65]'American Bar Association, CGL Exclusions for Cyberattacks and Loss of Electronic Data: Is There a Gap in Your Coverage? (2024).' Available at: https://www.americanbar.org/groups/tort_trial_insurance_practice/publications/the_brief/2019-20/summer/cgl-exclusions-cyberattacks-and-loss-electronic-data-there-gap-your-coverage/ (last visited Aug. 17, 2024).
[66]'American Bar Association, CGL Exclusions for Cyberattacks and Loss of Electronic Data: Is There a Gap in Your Coverage? (2024).' Available at: https://www.americanbar.org/groups/tort_trial_insurance_practice/publications/the_brief/2019-20/summer/cgl-exclusions-cyberattacks-and-loss-electronic-data-there-gap-your-coverage/ (last visited Aug. 17, 2024).
[67]Supra Note 36

This exclusion also applies to 'damages' for any expenses incurred by the policyholder, including expenses for credit monitoring, notification, forensic investigation, and legal research.

The Seventh Circuit has held that the data breach liability exclusion also does not apply to BIPA claims because it applies only to "situations in which hackers obtain access to personal information." Although BIPA does involve "disclosure" of information, its principal concern is disclosure to the policyholder, not to hackers who steal data from the policyholder.[68]

E. *Employment Practices Liability Policies and Biometric Data Privacy Claims*

Employment Practices Liability ("EPL") policies, which can be standalone or combined with other insurance coverages like Director & Officers ("D&O") Insurance coverage, may potentially provide coverage for biometric data privacy claims. These policies protect businesses against claims made by employees alleging violations of their legal rights by the company. If BIPA claims are considered employment-related practices, as insurers have argued when claiming that employment-related practices exclusions should prevent coverage for BIPA claims under CGL policies, then EPL policies should provide coverage because they specifically cover "employment practices wrongful acts."[69]

For the sake of an argument, let's assume a company uses biometric data, such as fingerprints, for employee timekeeping. If an employee sues the company for violating BIPA, the company might seek coverage under its EPL policy. However, the insurer could deny the claim if the policy has an exclusion for employment-related practices. In practice, insurers often deny claims for BIPA coverage under EPL policies. Hence, although EPL policies might offer coverage for biometric data privacy claims, insurers frequently reject claims for BIPA coverage under these policies.[70] As a result, businesses can be left vulnerable to substantial liability in the event of a lawsuit.[71]

[68] Supra Note 48
[69] 'Twin City Fire Insurance Co. v. Vonachen Services, Inc., 20-cv-1150-JES-JEH, United States District Court, Northern District of Illinois (2023).' Available at: https://casetext.com/case/twin-city-fire-ins-co-v-vonachen-servs (last visited Aug. 17, 2024).
[70]'Policyholder Pulse, Biometric Privacy, BIPA and the Battle for EPLI Policy Coverage (2024).' Available at: https://www.policyholderpulse.com/biometric-privacy-bipa-epli-coverage/ (last visited Aug. 17, 2024).
[71]'Corporate Counsel Business Journal, Managing Risk of Liability Stemming from Biometric Tech and Privacy Laws (2024).' Available at: https://ccbjournal.com/articles/managing-risk-of-liability-stemming-from-biometric-tech-and-privacy-laws (last visited Aug. 17, 2024).

F. *Disputes Over the Scope of EPL Coverage*

The case of Twin City Fire Insurance Co. v. Vonachen Services Inc.[72] ("Vonachen") highlights some potential coverage issues that may arise when relying on EPL policies for biometric data privacy claims coverage. In this case, Vonachen sought coverage to defend against class action lawsuits alleging that it violated BIPA when collecting employees' fingerprints for timekeeping purposes. The court found that the EPL coverage applied based on allegations by Vonachen employees that they were required, as a condition of employment set forth in the company handbook, to use the fingerprint-based timekeeping system and Vonachen failed to meet certain duties associated with fingerprint collection.

G. *Exclusions for Breach of Employment Contract*

Insurers may argue that biometric data privacy claims are excluded from coverage under EPL policies if the claims arise from a breach of employment contracts. However, the court found that an exception to the exclusion provision stating that it does not apply "to liability that would have been incurred in the absence of such contract" applied and did not bar coverage.[73]

H. *D&O Liability Insurance and Biometric Data Privacy Claims*

D&O liability insurance covers exposure faced by directors, officers, and the company itself that arise from actual or alleged wrongful acts. However, the policy exclusions in these policies differ and can create ambiguities in coverage for biometric data privacy claims.

For instance, a company's directors and officers are sued for invasion of privacy due to the company's collection and use of biometric data. If the company's D&O policy has an exclusion for claims based upon, arising from, or in any way related to any actual or alleged invasion of privacy, the insurer could deny coverage for this claim.

In the case of Vonachen, the D&O coverage did not cover losses related to any claim "based upon, arising from, or in any way related to any actual or alleged … 'invasion of privacy.'"[74] The insurer disputed coverage by arguing that the BIPA allegations in the underlying complaint related to an actual or alleged invasion of privacy. However, the court agreed that this exclusion

[72]Supra Note 69
[73]*Ibid.*
[74] III. Exclusions Applicable to All Insuring Agreements, *Ibid.*

barred coverage and stated that numerous cases have found a BIPA violation regardless of whether the underlying lawsuit uses the term "invasion of privacy." The court also rejected Vonachen's argument that BIPA violations occur only if the biometric information is collected surreptitiously or disseminated to third parties. While the court declined to find coverage under the policy's D&O provisions, it determined that there was coverage under the EPL provisions.

VI. LESSONS FOR INDIA

A. Regulatory Oversight of Biometric Data in India

In the Indian context, the governance of biometric data encompassing its collection, storage, and management is primarily under the purview of the Information Technology Act, 2000 ("IT Act"), and the rules promulgated thereunder.[75] The IT Act extends its regulatory reach to biometric data as it falls within the ambit of personal data processed via computer resources. Nonetheless, the IT Act, along with its subsidiary regulations, is predominantly centered on ensuring the security, integrity, and confidentiality of such data, rather than offering an exhaustive legal framework for digital personal data processing.

To address this lacuna, the DPDP Act was instituted, laying down a holistic legal structure for the handling of digital personal data. This Act acknowledges the dual imperatives of safeguarding individual rights to personal data protection and facilitating the lawful processing of said data. In light of the DPDP Act's implications, the Insurance Regulatory and Development Authority of India ("IRDAI") has convened a task force to scrutinize the Act's impact on the insurance industry.

The DPDP Act is India's first extensive law on personal data protection, covering all types of digital personal data, including biometric information. As the Act has not yet been fully implemented, the adequacy of its protections, especially concerning biometric data, remains untested. Thus, this situation calls for diverse interpretations and thorough evaluation from various viewpoints.

[75]For instance, rules like the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules of 2011.However, these Rules have been superseded by the DPDP Act. 'Ministry of Electronics and Information Technology, Government of India, GSR313E_10511 (2024).' Available at: https://www.meity.gov.in/writereaddata/files/GSR313E_10511(1)_0.pdf (last visited Aug. 17, 2024).

B. Regulation of Biometric Data under the DPDP Act

Biometric data, encompassing attributes such as facial features, fingerprints, and iris patterns, are unique identifiers intrinsic to individuals. Under the DPDP Act, although not classified as such explicitly, biometric data is considered personal data within the scope of informational privacy.[76] Consequently, the use and handling of biometric data are governed by the DPDP Act's provisions to mitigate risks such as data theft, misappropriation, and leakage.[77]

C. Government Use of Biometric Data

The Government of India leverages the Aadhaar system, recognized as the world's largest biometric platform, for nationwide identity verification.[78] The Aadhaar system facilitates the distribution of various government welfare services, subsidies, and benefits.[79] Notably, private entities are prohibited from using Aadhaar authentication or functioning as requesting entities to access individual information unless they meet certain requirements.[80]

D. Private Sector Handling of Biometric Data

Conversely, private entities are authorized to collect biometric information for business purposes. This data is stored and utilized by numerous organizations for various applications,

[76]Section 2(h) [defines, 'Data'], read with Section 2(t) [defines, 'Personal Data'] and Section 2(n) [defines, 'Digital Personal Data'] of the DPDP Act

[77]Statement of then Minister of State, Ministry of Electronics and Information Technology, Mr. Rajeev Chandrasekhar. 'Press Information Bureau, Press Release (2024).' Available at: https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1948357 (last visited Aug. 17, 2024).

[78]'Financial Express, Aadhaar now world's largest biometric database: 5 facts from UIDAI CEO's presentation in Supreme Court you must know (2024).' Available at: https://www.financialexpress.com/money/aadhaar-card-aadhaar-now-worlds-largest-biometric-database-5-facts-from-uidai-ceos-presentation-in-supreme-court-you-must-know-1108622/#:~:text=the Aadhaar scheme.-,A mammoth 1.2 billion or about 120 crore people have,Bhushan Pandey%2C revealed in his (last visited Aug. 17, 2024).

[79]'World Bank, Digital Dividends Aadhaar: Digital Inclusion and Public Services in India, Shweta Banerjee (2024).' Available at: https://thedocs.worldbank.org/en/doc/655801461250682317-0050022016/original/WDR16BPAadhaarPaperBanerjee.pdf (last visited Aug. 17, 2024).

[80]As per Section 4(4) of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, a private entity (i.e., a requesting entity not affiliated to the Central Government of India or the Government of any of the States in India) may be granted permission to perform authentication if the Authority is satisfied that the entity meets the following criteria:

(a) The private entity complies with the privacy and security standards specified by regulations; and
(b) (i) It is authorized to provide authentication services under any law enacted by Parliament; or
(ii) It is seeking authentication for a purpose prescribed by the Central Government, in consultation with the Authority, and in the interest of the State.

'The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, Act No. 18 of 2016 [25th March, 2016].' Available at: https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf (last visited Aug. 17, 2024).

including accessing public facilities, recording employee attendance, and securing digital assets through facial recognition or fingerprint scanning.[81]

E. Implications of the DPDP Act on Biometric Technology

Authentication of an individual's identity entails the collection, processing, sharing, storage, and eventual disposal of biometric data. The Supreme Court of India has mandated that government agencies and commercial entities demonstrate a "compelling State interest" for utilizing biometric data, emphasizing the significant impact on citizens' 'right to privacy'.[82]

F. Potential Shortcomings

The DPDP Act does not impose additional controls or requirements for processing personal data categorized under the GDPR as 'special category personal data'[83], the CCPA as 'sensitive personal information'[84], or under the erstwhile Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules of 2011 ("SPDI Rules") as 'sensitive personal data or information'.[85]Generally, this category includes data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for unique identification, and information concerning health, sexual life, sexual orientation, and religious beliefs.[86]

While the DPDP Act introduces a foundational framework for the protection of biometric data, it may not match the comprehensiveness of international data protection regulations such as the GDPR. The absence of additional controls or stringent requirements for processing biometric data could be viewed as a limitation of the DPDP Act. Additionally, the DPDP Act grants substantial discretionary powers to the Central Government in matters of data protection, including the authority to determine the scope and applicability of data protection provisions.[87]

---

[81]*Ibid.*

[82]'Supreme Court of India, Civil Original Jurisdiction, Writ Petition (Civil) No. 494 of 2012, Justice K.S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors. (24 August 2017).' Available at: https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf (last visited Aug. 17, 2024).

[83]'General Data Protection Regulation (EU) 2016/679, Art. 9 (2024).' Available at: https://gdpr-info.eu/art-9-gdpr/ (last visited Aug. 17, 2024).

[84] Section 1798.121, CCPA. 'California Civil Code, Division 3, Part 4, Title 1.81.5 (2024).' Available at: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 (last visited Aug. 17, 2024).

[85] Rule 3, SPDI Rules

[86]*Ibid.*

[87] Section 17(1)(c), read with Section 17(2), DPDP Act

This has raised apprehensions due to the absence of clear criteria or limitations, which could result in uncertainties and potential gaps within the regulatory framework.[88]

The Act's effectiveness in safeguarding biometric data will ultimately be assessed over time, through its practical implementation and enforcement.

VII. RECOMMENDATIONS FOR INDIA

Drawing on lessons from the U.S. model and addressing the gaps in the current legislative framework for personal data protection, India could consider certain enhancements to its regulatory system:

1. The enactment of targeted legislation or regulations that articulate clear guidelines for biometric data governance, coupled with enforcement provisions and penalties for non-compliance. For instance, the Government of India ordained the Security Guidelines for the use of Biometric Technology in e-Governance Projects ("Security Guidelines") of 2017.[89] These Security Guidelines provide a comprehensive framework for the protection of biometric information, ensuring its confidentiality, integrity, and availability during storage, processing, and transmission. Coupled with enforcement provisions such as regular audits and penalties for non-compliance, these measures would significantly enhance the security and privacy of biometric data in e-governance applications and systems in India;

2. The imposition of mandates on insurers to include biometric data privacy claims within the scope of cyber insurance policies, or the development of specialized insurance products catering to these risks. For instance:

    i. **Mandate Inclusion of Biometric Data Privacy Claims in Cyber Insurance Policies:** The IRDAI should consider requiring insurers to include coverage for biometric data privacy claims within their cyber insurance policies. This would

[88] For instance, under Section 2(f) of the DPDP Act, a child is defined as anyone under the age of 18, which complicates the implementation of digital access strategies for minors. Additionally, Section 9(1) of the DPDP Act mandates parental consent and age verification for data processing, however, this becomes challenging due to the extensive digital footprint of children in this age group. Consequently, this strict age-based definition may create issues with the feasibility of implementation and affect teenagers' autonomy, potentially leading to undue compliance burdens.

[89]'Government of India, Ministry of Electronics & Information Technology, Security Guidelines for use of Biometric Technology in e-Governance Projects (2024).' Available at: https://egovstandards.gov.in/sites/default/files/2021-07/Security Guidelines for use of Biometric Technology in e-Governance Projects.pdf (last visited Aug. 17, 2024).

ensure organizations have financial protection against liabilities stemming from breaches of biometric data;

ii. **Encourage Development of Specialized Insurance Products:** Additionally, Insurers should be encouraged to create specialized insurance products specifically addressing the risks associated with biometric data. These products could offer coverage for various scenarios, including data theft, misuse, and leakage;

iii. **Implement Robust Risk Assessment and Premium Calculation:** Insurers should develop comprehensive risk assessment mechanisms to evaluate the potential risks associated with an organization's handling of biometric data. This assessment should take into account the organization's data security measures, compliance with data protection laws, and the sensitivity of the biometric data they manage. The results of this assessment should then inform the calculation of insurance premiums; and,

iv. **Enhance Awareness and Education:** The IRDAI and other relevant authorities like the Ministry of Electronics & Information Technology of the Government of India should undertake initiatives to raise awareness about the importance of insurance coverage for biometric data privacy among businesses. This could involve organizing workshops, publishing educational materials, and offering consultation services to help businesses understand their potential liabilities and the benefits of adequate insurance coverage.

A. Insurance Coverage Considerations

In the U.S., CGL policies often incorporate exclusions pertaining to employment practices, which may preclude coverage for personal and advertising injuries linked to employment-related activities. The applicability of such exclusions to BIPA claims has been a subject of judicial divergence. In India, analogous exclusions exist, yet their relevance to biometric data privacy claims remains to be clarified.

Moreover, certain U.S. CGL policies exclude coverage for personal and advertising injury claims associated with statutory infringements. In India, while indemnities in contracts are not subject to statutory limitations on loss quantum, the implications for biometric data privacy claims are yet to be determined.

EPL and D&O insurance in the U.S. may potentially cover biometric data privacy claims, protecting businesses against employee allegations of legal rights violations. The potential for analogous coverage under Indian insurance policies warrants examination.

B. Optimal Strategies and Business Practices for Coverage of Biometric Data Privacy Claims

i. Evaluating the Risk of Claims

When seeking insurance coverage for claims and costs related to biometric data, organizations should first evaluate the risk of facing a violation or claim under biometric data privacy law.[90] This involves identifying the biometric data they collect and understanding the laws that apply to this data, including any data disclosed or outsourced to third-party vendors. Organizations should also consider the additional liability they may face from private lawsuits when selecting coverage, subject to the applicable regulatory requirements. To accurately identify and assess the risk of biometric data privacy claims, organizations should gather information from various stakeholders, including departments or offices responsible for:

- Information technology and information security;
- Privacy or compliance;
- Human resources;
- Business operations, including product or service development; and,
- Legal risk.[91]

This interdisciplinary approach is crucial to assess the organization's risk profile for biometric data privacy claims and determine the necessary coverage. By evaluating the risk of claims, businesses can better understand their potential liabilities and take steps to mitigate these risks. Such an approach can help businesses avoid costly legal disputes and ensure they have adequate insurance coverage.

[90]For instance, on May 18, 2023, the U.S. Federal Trade Commission released a policy statement cautioning that the increasing use of technologies involving biometric information poses potential risks to consumer privacy and data security, as well as the potential for bias and discrimination. The FTC clarified that biometric information technologies encompass all technologies that utilize or claim to utilize biometric data for any purpose. 'Davis Wright Tremaine LLP, Biometric Policy Statement (2023).' Available at: https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/06/p225402biometricpolicystatement.pdf?rev=bfa4f92b7ac2476681ce505725bf3b69&hash=14A7B0C218858CF5718A7F70EFDA2F0C (last visited Aug. 17, 2024).

[91]'International Risk Management Institute, Claim Evaluation: Determining Valuation (2024).' Available at: https://www.irmi.com/articles/expert-commentary/claim-evaluation-determining-valuation (last visited Aug. 17, 2024).

ii. Reviewing Current Policies

Organizations should scrutinize their existing policies to ascertain whether they cover biometric data privacy claim costs and identify any exclusionary language that may prevent coverage. Insurance coverage disputes often hinge on a few keywords within a policy. Therefore, organizations should ensure their policy language offers adequate protection by:

- Analyzing all potential biometric data privacy claim scenarios against the policy language;
- Identifying all ambiguous language and provisions in each policy;
- Reviewing all definitions in each policy to ensure they encompass biometric data privacy claims;
- Ensuring that the organization understands and can comply with each policy's terms and conditions; and,
- Reviewing all exclusions to ensure that they do not prevent biometric data privacy claims coverage.

Organizations should engage specialized legal counsel to review their policies for potential coverage gaps for biometric data privacy claims. If necessary, organizations should negotiate better coverage terms (or remove or revise potentially troublesome exclusions) at either policy issuance or renewal. Many organizations use insurance brokers to assist in placing their policies. While brokers do not practice law, they can help identify what terms specific insurers have agreed to in the past. Although organizations often successfully seek coverage for biometric data privacy claims under traditional insurance policies, they may encounter insurer challenges to coverage based on the policy terms, conditions, and exclusions. In many cases, a stand-alone cyber policy may be the best solution to ensure broad coverage. Organizations should also monitor ongoing litigation concerning biometric data privacy claims coverage.

iii. Understanding the Selection of Choice of Law

Subject to the jurisdiction, substantive law governs insurance disputes, and the substantive laws vary significantly from country to country (or, State to State, as is the case in the US jurisdiction).[92] A court's interpretation of insurance contract language can mean the difference

[92]'Transnational Law Blog, A Primer on Choice of Law Clauses (2024).' Available at: https://tlblog.org/a-primer-on-choice-of-law-clauses/ (last visited Aug. 17, 2024).

between a coverage victory or loss. Organizations should work with counsel to examine the best forum and choice of law for litigating coverage disputes.[93] If insurers try to add specific choice of law provisions, organizations should ensure they understand the ramifications of that choice. Understanding the choice of law provisions in their policies can help businesses anticipate how potential disputes might be resolved. This can inform their risk management strategies and help them select the most advantageous coverage options.

VIII. CONCLUSION

The intersection of insurance policies and biometric data privacy presents increasingly complex challenges as technology advances and regulations evolve. This research sheds light on the intricate nature of statutory exclusions within CGL policies and the varied interpretations by courts, particularly concerning the BIPA in the United States. Cases like Krishna Schaumburg highlight the ongoing judicial debate over the applicability of these exclusions, emphasizing the need for clearer policy language and more explicit legal guidance.

EPL and D&O insurance policies present potential avenues for covering biometric data privacy claims. However, their effectiveness is often compromised by exclusions and ambiguities. The Vonachen case, for example, illustrates the nuanced challenges organizations encounter when seeking coverage under these policies, especially when biometric data collection intersects with employment practices.

In India, the governance of biometric data is primarily directed by the IT Act and the recently enacted DPDP Act. While these regulations provide a foundational framework, they may not be as comprehensive as international standards (such as the BIPA or the GDPR). This presents an opportunity for India to strengthen its regulatory approach by learning from the U.S. model and addressing identified shortcomings.

The research suggests that organizations should proactively evaluate their insurance coverage for biometric data privacy claims. This involves conducting a thorough risk assessment, carefully reviewing existing policies, and strategically selecting coverage options. As biometric data becomes increasingly integral to both the private and public sectors in India, it is crucial

[93]'WilmerHale, Choice-of-Law Agreements in International Contracts (2024).' Available at: https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/documents/20211217-choice-of-law-agreements-in-international-contracts.pdf (last visited Aug. 17, 2024).

for regulatory frameworks and insurance policies to evolve in tandem, providing robust protection against emerging risks.

To address these challenges, the research recommends targeted legislative actions and reforms within the insurance industry in India. This includes incorporating biometric data privacy claims into cyber insurance policies and developing specialized insurance products. Such measures would help bridge the current regulatory gaps, ensuring that businesses and individuals are adequately protected in an increasingly digital world. While India has made significant strides in regulating biometric data, persistent gaps in its regulatory framework remain. By adopting best practices from the U.S., India can strengthen its legal protections and enhance the privacy rights of its citizens.

RECONCEPTUALIZING CORPORATE FIDUCIARY OBLIGATIONS WITH AI PERMEATION

—Abhishri Marda[*]

ABSTRACT

Owing to the nature of control exercised by a director over the company, the former acts as a fiduciary for the beneficial interest of the latter. This paper aims to understand how fiduciary duties in the age of Artificial Intelligence (AI) permeation would be reconceptualized if AI is incorporated into the boardroom. The paper argues that despite the conceivability of artificial intelligence being able to independently carry out fiduciary obligations without intervention of human directors, there lay certain key obstacles in designating the post of fiduciary to AI on its own. Hence, the only way of incorporation of AI into the boardroom is not through unsupervised delegation but through assisted intelligence wherein the perfect balance is struck through the creation of mixed boards by complying with the legal framework governing directors and delegation while meeting superior governance demands.

In incorporating assisted intelligence into mixed corporate boards, this paper advocates for certain ethical standards so as to maintain the observance of openness and fairness in practice which is to be codified at the outset. Such standards must be inspired and superimposed from the European Union's AI regulation to the Indian Company Law framework. Once the same is achieved, it is argued that the doctrine of respondeat superior must be invoked so as to impose fiduciary liability on the principal directors making use of agent AI systems in carrying out their corporate obligations. This paper envisions the reconceptualization of corporate fiduciary duty by not relieving the

[*] The author is a student at Jindal Global Law School, O.P. Jindal Global University (JGLS).

traditional fiduciaries of their obligations simply by virtue of reliance upon AI in the boardroom.

I. INTRODUCTION – THE INSPIRATION INFORMING FIDUCIARY LAW

The interpretation of the word "fiduciary" under modern law is to incorporate all trust-like situations, more precisely, in direct contradiction with trusts proper, encompassing situations which are trust-like in certain respects but not by strict definition trusts.[1] Fiduciary law encompasses those crucial relationships of trust and confidence resulting in one party's implicit dependency and distinctive vulnerability in relation to the other within circumscribed limitations and the main task is to impose strict obligations based on the foundations of the utmost good faith on fiduciaries, including the duty to act honestly, selflessly so as to avoid conflict of interests, with integrity, and in the best interests of their beneficiaries.[2] Fiduciary law exists as one of the primary forces ensuring the contemporary relevance of equity by allowing certain classes of individuals to trust that their interests will be cared for by their respective fiduciaries in a relationship of interdependency and vulnerability.[3] Within a company law framework, the director being the fiduciary owes it to the company due to the extent of control exercised by the former over the latter, and consequently, it is the duty of directors to act in the company's best interest and awareness.[4] In *Nanalal Zaver and Another v Bombay Life Assurance Company Limited and Others*, it was established that when the director acts against the interest of the company, court intervention would be justified by the fact that the relationship between the director and the company resembles the relationship of a trustee and of a cestui que trust i.e. the beneficiary. [5]

II. THE PREVAILING UNDERSTANDING OF FIDUCIARY DUTIES UNDER COMPANY LAW

In *Ferguson v Wilson d*irectors have been held to be agents of its principal company, which cannot act by itself, but only through its agents.[6] The directors of a company as its agents must

[1] L. S. Sealy, 'Fiduciary Relationships' (1962) *20*(1) The Cambridge Law Journal 69,72 <https://heinonline.org/HOL/P?h=hein.journals/camblj1963&i=131> accessed 25 March 2024.
[2] Leonard I. Rotman, 'Understanding Fiduciary Duties and Relationship Fiduciarity' (November 28, 2017). 62(4) McGill Law Journal 977, 986 <https://ssrn.com/abstract=3078806> accessed 25 March 2024.
[3] Rotman (n 2) 987.
[4] Vijay P Singh, 'Directors' Fiduciary Duties to the Company: A Comparative Study of the UK and Indian Companies Act' (2021) 27(1-2) *Trusts & Trustees* 132, 140 <OP-TANT200121 132..150 (silverchair.com)> accessed 25 March 2024.
[5] *Nanalal Zaver and Another v Bombay Life Assurance Company Limited and Others* 1950 SCR 391, para 54.
[6] *Ferguson v Wilson* [1866] 11 WLUK 32.

act ethically in advancing objectives and interest of their principal and must pursue beneficial goals in the exercise of their knowledge of expertise with reasonable care and in a bonafide manner so as to accomplish positive outcomes and growth for the company.[7] Further it was established in *Cede & Co. v. Technicolor* that directors must abide by the three pillars of good faith, loyalty, and due care toward the corporation in the exercise of their duties. [8] Although the Companies Act, 2013 makes no reference to the use of artificial intelligence mechanisms by a director in the performance of his obligations, the fiduciary duty of the director is contained within section 166(2) and (3) wherein *a director shall act in good faith in the best interests of the company and shall exercise his duties with due and reasonable care, skill and diligence and independent judgement.* [9] The increasing pervasiveness of AI mechanisms in everyday decision-making including in diversified professional domains gives rise to the question about the possible reconceptualization of fiduciary duties within a company so as to include AI as a fiduciary or in marking the evolution of the fiduciary obligations of the director in a hypothetical future consisting of AI-assisted decision-making by the Board of Directors.

III. CAN ARTIFICIAL INTELLIGENCE BE TREATED AS AN INDEPENDENT FIDUCIARY BY ITSELF?

The most advanced form of artificial intelligence is automation wherein Al takes over all the powers including the final decision-making authority, operating without any human intervention, and thus, this stage of automation is where human directors would be substituted by AI and the question of the fiduciary capacity of AI as an entity in itself would materialize.[10] Like human fiduciaries, artificial fiduciaries would be required to make decisions in the best interest of the company and thus an understanding of loyalty similar to a human understanding is to be programmed.[11] The equitable concept of fiduciary duty is meant to avoid, regulate, and minimize the intrinsic conflict of interests prevalent in the relationship between a human agent and a human principal.[12] Bias arises when results are produced by an AI that are systematically

[7] Singh (n 4) 135.
[8] *Cede & Co. v. Technicolor, Inc.* 634 A.2d 345 (Del. 1993).
[9] The Companies Act, 2013 s 166(2) and (3).
[10] Aashirwa Baburaj, 'Artificial Intelligence v. Intuitive Decision Making: How Far Can It Transform Corporate Governance?' (2021) 8 GNLU L. REV. 233, 243 <https://heinonline.org/HOL/P?h=hein.journals/gnlur8&i=257> accessed 24 March 2024.
[11] Zhaoyi Li, 'Artificial Fiduciaries' (2023) 81(4) Washington and Lee Law Review, Forthcoming 1,42 <delivery.php (ssrn.com)> accessed 26 March 2024.
[12] Anat Lior, 'AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy' (2020) 46 MITCHELL HAMLINE L. REV. 1043, 1091 <https://heinonline.org/HOL/P?h=hein.journals/wmitch46&i=1043> accessed 26 March 2024.

prejudiced because of erroneous assumptions fed into the machine learning process.[13] Since the same is programmed by a natural person there would be a strong connection between the logic of the developer and the logic of his creation as following aspects of human logic and intention of the former thus as long as it is not programmed to devise its own objectives or conditioned by the biases of its maker, it is possible to subvert automation bias.[14] Al will lack independent will to act on biases or learn from its surroundings and replicate biases if these abilities are not created in the first place by the developer by direct, or indirect, commands and/or algorithms either at the time of creation or during processing[15] and thus checks need to be maintained so as to monitor what is being fed into the AI. The concerns regarding advanced AI's inability in fulfilling the loyalty requirement towards the beneficiary associated with the post of a fiduciary are motivated by the fact that the objective acquired by the AI system might not be identical to the goal of the entity deploying the same.[16] However, the property rights natural persons hold over artificial intelligence so as to possess, use and dispose AI guarantee human control overriding any autonomy of AI in being able to advance its personal goals.[17] In reality, AI being designed without any biases would carry the potential of simulating the role of an independent director by being able to accomplish the goal of fairness by being unsusceptible to any conflicts of interests[18] and thus could prove to be more loyal to the company than individual directors. Furthermore, it carries the potential to mitigate information asymmetry and enhance transparency in boardrooms by increasing accessibility to information through its ability to store and process massive amounts of data.[19]

Despite the conceivability of artificial intelligence being designed in a way so as to be able to independently carry out fiduciary obligations towards the company, there lay certain key obstacles in designating the post of fiduciary to AI on its own. S. 2(34) of the Companies Act, 2013 defines a director as "any *person* appointed to the Board of a company" [20] and thus it follows that under the prevailing legal regime only a natural person is capable of holding the

[13] Michael R. Siebecker, 'Making Corporations More Humane through Artificial Intelligence' (2019) 45 J. CORP. L. 95, 145 < https://heinonline.org/HOL/P?h=hein.journals/jcorl45&i=105> accessed 27 March 2024.
[14] Aleksei Gudkov, 'On Fiduciary Relationship with Artificial Intelligence Systems' (2020) 41(25) LIVERPOOL L. REV. 251, 256 < https://heinonline.org/HOL/P?h=hein.journals/lvplr41&i=251> accessed 25 Mach 2024.
[15] Gudkov (n 14) 257.
[16] Claire Boine, 'Fiduciary law to promote value alignment in AI systems' (2020) We Robot 2020 1,6 <Fiduciary-paper.pdf (bu.edu)> accessed 26 March 2024.
[17] Gudkov (n 14) 256.
[18] Baburaj (n 10) 246
[19] Baburaj (n 10) 247.
[20] The Companies Act, 2013 s. 2(34).

office of a director. The corporate fiduciary that even introduces AI as a fiduciary by itself will also contravene the statutory and common law requirements that place stringent limitations on the ability of the fiduciary to delegate their fiduciary obligations.[21] The same gets reflected under s. 166(6) of the Companies Act, 2013 wherein a director **CANNOT** assign or delegate his office to any other, and any such delegation is void. [22] Furthermore, one of the most instrumental features underlying all fiduciary relationships is identified to be the availability of the same remedy against the wrongdoer fiduciary on behalf of the beneficiary as would exist against a trustee on behalf of the cestui que trust.[23] The fundamental limitation of AI being capable of acting as a fiduciary is the absence of a legal personality rendering it impossible for AI to be held legally liable in its own capacity.[24] Thus, the absence of legal mechanisms to curb bias, statutory limitations defining directors and restraining delegation of their office, and the additional difficulty of AI lacking the ability to sue and be sued due to lack of its individual legal personality are the key hinderances in its social recognition as a fiduciary.

IV. THE ALTERNATIVE FOR INCORPORATING AI

Assisted intelligence contemplates entrusting AI with carrying out specific tasks that may assist the Board of directors in making certain decisions wherein the power to make decisions is not delegated to the Al, rather the output given by it is relied upon by the final decision-making authority, the human director.[25] It might become a routine practice to employ AI to facilitate the board's decision-making expertise by analyzing data and market trends and in determining allocation of funds so as to harmonize the overarching objectives of the company.[26] This mode of incorporation achieves a perfect equilibrium through embracing consultation by balancing AI's quantitative efficacy in processing data beyond human capacities and a human's ability of qualitative analysis.[27] Assisted decision-making is permissible under the prevailing law since neither does it involve any delegation of power and nor does AI as an artificial entity

[21] Alfred R. Cowger Jr., 'Corporate Fiduciary Duty in the Age of Algorithms' 14(2) Case Western Reserve Journal of Law, Technology & the Internet (2022– 2023) 136,182 <Corporate Fiduciary Duty in the Age of Algorithms (case.edu)> accessed 29 March 2024.
[22] The Companies Act, 2013 s 166(6).
[23] Sealy (n 1) 73.
[24] Gudkov (n 14) 266.
[25] Baburaj (n 10) 241.
[26] Else, Shani R., and Francis G.X. Pilegg, 'Corporate Directors Must Consider Impact of Artificial Intelligence for Effective Corporate Governance' (2019) Business Law Today (February 2019) 1,6 <https://www.jstor.org/stable/27180364> Accessed 25 March 2024.
[27] Baburaj (n 10) 251.

occupy a seat in the boardroom so as to replace the human director.[28] The incorporation of assisted decision-making AI within the boardroom would give rise to the creation of mixed boards retaining the "appointed natural person" director mandate as envisioned under s. 2(34) of the Companies Act, 2013 while paving the road for more efficacious and comprehensive decision-making by leveraging and maximizing the advantages of AI developments. Hence, it follows that mixed boards could adequately comply with the current legal framework mandating human directors and capitalize on AI developments so as to facilitate superior governance demands.[29] Furthermore, with artificial fiduciaries joining the board of the company, the same would be accompanied with changes in the duty of care of human fiduciaries on mixed boards so as to govern their treatment of suggestions by their AI counterparts.[30]

The duty of care is further divided to include two fiduciary obligations of exercising the 'requisite degree of care in the process of decision making', and to 'act on an informed basis' so as to consider all accessible and relevant information prior to making decisions.[31] One of the major benefits of corporate fiduciaries consulting AI is the efficacy and comprehensiveness accomplished through the colossal magnitude of data processing and translating into manageable chunks so as to enable directors to thoroughly analyze relevant data and make accurate predictions.[32] A paradoxical fiduciary duty of care dilemma would arise which could create a loophole for directors so as to evade accountability.[33] The paradox would entail the obligation to employ the best and latest AI tools so as to enable the most efficacious and skilled decision making and any dereliction in this contemporary mode of discharge of obligation of consulting AI would be considered to be afoul of the expected diligence and loyalty of a director towards advancing the interests of the beneficiary company. [34]Simultaneously, if the directors make use of AI tools without paying heed to the opacity of decisions due to black box processing so as to mindlessly delegate decisions without understanding the underlying process

[28] Baburaj (n 10) 252.
[29] Li (n 11) 40.
[30] Li (n 11) 39.
[31] Rudresh Mandal and Siddharth Sunil, 'The Road Not Taken: Maneuvering Through the Indian Companies Act to Enable AI Directors' (May 28, 2020) 1,12 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3855415> accessed 29 March 2024.
[32] Cowger Jr. (n 21) 158.
[33] Baburaj (n 10) 252.
[34] Cowger Jr. (n 21) 156.

or justification would create a claim for violation of the duty of care.[35] A suggestion to tackle such a paradox would be to not ascribe the standard of care, in general, to the employment of AI to supplement decision-making but to assess whether there lies any justification behind the use of AI in making decisions in a particular scenario thereby to impose a standard of care on the directors using such AI. [36]

V. LEARNING FROM EU'S AI REGULATION TO SECURE ETHICAL USAGE

The potential biases that AI may carry gives rise to certain ethical standards requiring compliance so as to maintain bonafide corporate governance. These ethical standards can be imposed by taking inspiration from and superimposing certain provisions of the EU AI Regulation. At the very outset, although it is possible that AI may be contaminated by biases the same is contingent upon the nature of data fed into it and the question of bias arises only in a situation when the integrity of the data is under suspicion.[37] To tackle such a possibility of automation bias, a provision resembling Article 14 of the EU regulation could be made so as to ensure that human oversight is still maintained[38] by the directors (acting in furtherance of their due diligence and duty of care obligations) by way of keeping a check on the veracity and comprehensiveness of the data being processed by AI that is relevant to their expertise as directors, and to halt any decision-making based on the conclusions reached by it till a sound judgment of unbiasedness is arrived at first. Drawing inspiration from Article 29(6b)[39] without delving into the intricacies of what high-risk AI systems are as contemplated under the Act there exists a need to create new uniformly applicable provision that the employers of AI systems being used to make decisions or assist in making decisions related to natural persons (the shareholders, and other stakeholders in the company law context) shall, in order to maintain transparency, make disclosures to the natural persons that their confidence is subject to the use of the AI. Transparency would ensure that information about the company's operations and governance is easily accessible to various stakeholders through mandatory disclosure which would also be in furtherance of curbing information asymmetry. [40] Such a disclosure is to include the intended purpose that the AI was designed for, the specific context

[35] Cowger Jr. (n 21) 156.
[36] Baburaj (n 10) 252.
[37] Baburaj n (10) 245.
[38] Council Regulation 5662/24 (EC) of 26 January 2024 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative act art 14.
[39] Council Regulation 5662/24 (EC) of 26 January 2024 art 29(6b).
[40] Baburaj (n 10) 247.

and conditions of its use as defined under Article 2(12) and the type of decisions made in furtherance of the same.[41] It also includes notifying the natural person about their right to an explanation as provided under Article 68c so as to provide a basis for the affected individuals to exercise their rights[42] in case of any deviation from the intended purpose and to act as a tool for imposing liability.

VI. CONCLUSION - DETERMINATION OF AI'S FIDUCIARY LIABILITY

Although AI, if programmed to be fair and compatible with the goals of the company unlike directors, is incapable of committing fraud due to a lack of insidious ulterior networking, an additional channel for evasion of liability by directors arises by citing AI as an excuse due to the likelihood of courts not holding AI liable on account of execution difficulties.[43] Such a loophole is likely to be misused as a mitigating factor on account of prevailing discourse concerning the enhanced duty of care obligations including but not limited to using the appropriate AI, considering its suggestions and to attain a balance in the paradox of mandatory use of AI so as to facilitate superior decision making but to not breach the principle of *delegatus non-potest delegare*. Furthermore, since the legal personhood of Al is not accorded statutory or judicial recognition, the fiduciary duties owed by it and any claims imposing liability stand reposed on the director who is the human-operator.[44] With AI ensuring superior and more comprehensive decision making through the use of efficacious tools, directors could conveniently defend themselves by stating that their fiduciary duty of care has not been violated, thus enabling them to abandon liability through blanket dependence on Al which can prove to be problematic if the level of qualitative judgment and intervention as required is not undertaken. The most appropriate solution in such a contingency is the application of the *doctrine of respondeat superior* creating a fictional relationship of principal and agent between the director and AI so as to enable the director to be better equipped to regulate and adjust the levels of activity of the Al agent and to be answerable to the liability claims arising through the use of AI.[45]

[41] Council Regulation 5662/24 (EC) of 26 January 2024 art 2(12).
[42] Council Regulation 5662/24 (EC) of 26 January 2024 art 68c.
[43] Li (n 11) 59.
[44] Gudkov (n 14) 267.
[45] Lior (n 12) 1097.

Al lacks the ability to assume liability and thus the only entity on which liability may be imposed is the human principal director(s) pulling its strings so as to benefit from it and thus would be held primarily liable with respect to the actions of its AI agents.[46] The *doctrine of respondeat superior* in corporate liability would superimpose what is done for employee misconduct to algorithmic or AI misconduct.[47] Thus, analogous to when employee action is attributable to the company and thus by extension the director, the doctrine effectively enquires whether a company had control over and could expect to benefit from their employee's activity and thus AI action would be attributable to the company only when the corporation has control over and claims the benefits of the AI.[48] The programmer may not be held liable since AI subsequent to being programmed is capable of acting independently and does not fulfill the act done within the scope of employment requirement[49] but in the case of the director, the Al agents lack the ability to act independently and to further any purpose not corresponding to its employer given the control exercised by its human principal director over what tasks are assigned and when.[50] Additionally, since the only reason AI is employed is owing to its productive efficacious and comprehensive nature of processing and decision-making as a corporate resource[51], the directors can be said to be directly benefitting from the activity of AI in furthering their own responsibilities. Thus, corporate fiduciary duty of care and due diligence in the future's AI permeated society is reconceptualized by holding the principal directors strictly liable when reaping the benefits of AI for its Al agents' misconducts so as to incentivize the assurance and use of a safer algorithmic environment. [52]

[46] Lior (n 12) 1100.
[47] Mihailis E. Diamantis, 'Algorithms Acting Badly: A Solution from Corporate Law' (2021) 89 Geo Wash L Rev 801, 849 <https://heinonline.org/HOL/P?h=hein.journals/gwlr89&i=857> accessed 5 April 2024.
[48] Diamantis (n 47) 849.
[49] Daniela Vacek & Matteo Pascucci, 'Vicarious Liability: A Solution to a Problem of AI Responsibility?' (2022) 24(3) Ethics and Information Technology 1,12 <Vicarious Liability: A Solution to a Problem of AI Responsibility? (researchgate.net)> accessed 5 April 2024.
[50] Lior (n 12) 1099.
[51] Diamantis (n 47) 844.
[52] Lior (n 12) 1102.

DEEPFAKES AND DIGITAL ETHICS: GLOBAL CHALLENGES AND INDIA'S ROADMAP FOR REGULATION

—Ishan Ranjan[*]

ABSTRACT

Deepfakes, a portmanteau of "deep learning" and "fake," represent an advanced yet controversial technological frontier. This paper explores the dual-edged nature of deepfake technology: its groundbreaking capabilities and the profound societal challenges it presents. Deepfakes use artificial intelligence and machine learning to produce content that mimics authentic appearances, often convincingly replicating speech or actions. While the technology holds potential for societal benefits—such as giving a voice to individuals who have lost theirs due to medical conditions—it also poses serious threats. These include copyright infringement, fraud, defamation, identity theft, and risks to national security. The paper adopts a comprehensive approach, examining the mechanisms behind deepfakes, their societal advantages, and the ethical dilemmas arising from misuse. It reviews current detection methods, which strive to counteract even the most sophisticated deepfakes that can deceive experts. Additionally, it assesses the legislative responses of countries like China, the USA, the UK, the EU, and India, focusing on regulations against unauthorized AI-generated content and its dissemination. The societal and moral implications, including the erosion of trust in electronic media, are critically analyzed. The paper argues for India's need to craft legislation that aligns with its constitutional principles while addressing the unique challenges posed by deepfakes. Using a mixed-method research approach, the study incorporates primary data from a diverse age-based survey alongside secondary sources, including

[*] The author is a student at School of Law, Christ University, Bengaluru.

legal analyses and expert opinions. Ultimately, the paper aims to provide a global perspective on deepfake implications while advocating for India to establish robust, principled regulations to mitigate the technology's adverse effects.

Keywords: deepfake, artificial intelligence, India, legislations.

I. INTRODUCTION

Deepfake is a technological achievement that lets any user digitally create any action, be it audio, video, or speech, by another person, which that person has not performed in real life. It is a complement to the growth in the field of artificial intelligence and machine learning, as it is majorly backed by the same as its fundamental algorithm. The development of deepfakes has achieved such remarkable feats that it has become challenging for humans, let alone experts. It gathered the world's attention when a deepfake video of US ex-president Barack Obama was posted on YouTube, where he seemed to talk about the rising concern about disseminating misinformation and its harms and struggles. Although the video was supposed to be an irony to the situation, it can be used and misused in many unimaginable ways by the unending expansion of the human brain's capabilities.

A deepfake might not necessarily be in an audio-video format where a person is seen speaking and doing something, though it is the most common form. There are other methods, such as audio and image generated with such precision that it may easily deceive any ordinary human eyes. This was seen in 2019 when the CEO of a UK-based company was scammed off USD $243,000 over a synthetically produced phone call, which perfectly replicated one of the chief executives of the company's German-based parent company.[1]

Although, more often than not, it is supplemented with illicit gains and unlawful behaviors such as fraud, dissemination of misinformation, generating fake pornography, etc., it is not always used as an evil means of criminal activities, such as giving people who have lost their

[1] *Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company* [Online]. Trend Micro (MX). Available at: https://www.trendmicro.com/vinfo/mx/security/news/cyber-attacks/unusual-ceo-fraud-via-deepfake-audio-steals-us-243-000-from-u-k-company (Accessed: 24 November 2024).

voice due to several medical conditions, to virtually speak again by companies such as VocaliD.

II. RESEARCH METHODOLOGY

This study employs a mixed-method research approach, combining both qualitative and quantitative methodologies to provide a comprehensive understanding of the deepfake phenomenon and its regulatory landscape. The primary quantitative component consisted of a survey designed to assess the public's ability to detect AI-generated deepfake content. The survey instrument presented participants with a carefully curated set of 20 images, equally divided between authentic photographs and AI-generated deepfakes. Participants across different age groups were asked to identify which images were real and which were artificial, providing a measurable metric of deepfake detection capability. The survey results yielded an average score of 10.42/20, with scores ranging from 6 to 15, and a median score of 10/20, challenging the initial hypothesis that the 18-25 age group would demonstrate superior detection abilities due to their technological familiarity. The qualitative aspect of the research involved a comprehensive analysis of existing legislative frameworks across multiple jurisdictions, including the United States, China, the United Kingdom, the European Union, and India. This analysis encompassed a detailed review of primary legal sources, including statutes, regulations, and policy documents, supplemented by secondary sources such as academic literature, expert opinions, and legal commentaries. The study also incorporated analysis of significant deepfake incidents, such as the UK-based company's financial fraud case and the Tamil Nadu political campaign incident, to provide real-world context to the theoretical framework. Documentary analysis was conducted on emerging legislation such as the No AI FRAUD Act, the Digital Personal Data Protection Act, 2023, and the EU's AI Act, examining their approach to regulating deepfake technology. The research methodology was designed to bridge the gap between theoretical understanding and practical implementation of deepfake regulation, while also measuring public awareness and detection capabilities. This dual approach allowed for a more nuanced understanding of both the technical and social dimensions of the deepfake challenge, providing a solid foundation for policy recommendations and future research directions.

III. TECHNICAL FRAMEWORK AND OPERATIONAL MECHANISMS OF DEEPFAKE TECHNOLOGY

Deepfakes, although rely primarily on artificial intelligence for their functioning, there exist further methods involving AI with intricate differences that separate one from the other and make them unique.

Variational autoencoders, or VAE, consist of two parts: an encoder and a decoder. The data regarding a person, such as an accent, body language, mannerisms and behaviours, voice modulation, and tone, etc., are fed to the computer, where the encoder breaks down these data and information in a lower-dimensional latent representation, which the decoder takes up to reconstruct to imitate the individual's actions.

Generative adversarial networks (GANs) consist of two networks designed in a fashion where each one competes to beat the other in a "game." The Generator creates outputs regarding the individual's appearance and mannerisms, and that output is examined on its accuracy by the other network, which is the discriminator. The former then improves its production based on the feedback from the discriminator, which compares the output with the original videos to provide the evaluation.

Diffusion Models (DM) is a comparatively newer method where an artificially intelligent software moderately adds noise to data in order to train itself by subsequently producing outputs and then reverses the model to generate the final result in the form of a deepfake.

Identifying deepfake-generated content can be difficult for an ordinary human being, let alone experts, although there could be many giveaways in such content. For example, in a deepfake-generated video, uncanny mannerisms, little to no blinking of eyes, non-alignment of speech to facial expressions, and certain other flaws in the body language of the person seen in the video can act as giveaways regarding the legitimacy of the content. In an experiment conducted, it was found that when a warning label is not given to the viewers of a deepfake, their chances of figuring out the fact that they have been exposed to a fake video was only 32.9%. Additionally, when a warning label was, in fact, given, the detection capability of the

viewers went up to 21.6% from 10.7%.[2] The results show that a person has an inclination to find out if they are being exposed to fake AI-generated content if they are being told that there is a chance of it being fake. Thus, they must rely on the policies and legislation for content moderation.[3]

Technicians often rely on specific data algorithms to ease their tasks and increase their chances of success. These algorithms attempt to detect the digital fingerprints of AI-generated content with its existing database and compare it with already existing content in the digital environment. Advanced techniques also analyses biological signals, like heart rhythms, that deepfake can't replicate yet.

IV. LEGAL IMPLICATIONS AND JURISDICTIONAL CHALLENGES OF DEEPFAKE PROLIFERATION

To understand the various possible legal consequences of deepfakes, we have to comprehend the various types of content that can be generated as deepfakes with the help of artificial intelligence. Such content can vary from a very genuine-looking email or a text message to a very convincing video of a person or a phone call with a synthetic voice of a human being as a sham of someone else.

There have been more than enough instances across the globe to convince us of the harmful repercussions of deepfakes. Such instances include finance workers being scammed of USD $25 million through a video conference with a deepfake CFO of the company.[4] For election campaigns in India, the political parties in Tamil Nadu began virtually resurrecting their dead political leaders through deepfake videos, which acted as a part of their respective campaigns.[5] Revenge pornography has become another major and widespread evil form of deepfakes. It involves masking an individual's face on pornographic content, oftentimes linked to ulterior

[2] Lewis, A., Vu, P., Duch, R.M. and Chowdhury, A., 2022. Do content warnings help people spot a deepfake? Evidence from two experiments. *OSF Preprint*.

[3] (2022). *Do Content Warnings Help People Spot a Deepfake? Evidence from Two Experiments* [Online]. Available at: https://royalsociety.org/-/media/policy/projects/online-information-environment/do-content-warnings-help-people-spot-a-deepfake.pdf (Accessed: 29 November 2024).

[4] H. Chen, (2024). *Finance worker pays out $25 million after video call with deepfake 'chief financial officer'* [Online]. CNN Business. Available at: https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html (Accessed: 27 November 2024).

[5] N. Christopher, (2024). *How AI is resurrecting dead Indian politicians as election looms* [Online]. Al Jazeera. Available at: https://www.aljazeera.com/economy/2024/2/12/how-ai-is-used-to-resurrect-dead-indian-politicians-as-elections-loom (Accessed: 27 November 2024).

reasons such as extortion or revenge. Such generated content is then disseminated on the web if the demands of the person creating them are not met with or cause reputational damage to an individual. Many such deepfakes of global celebrities have been circulated on the internet, such as Taylor Swift, Priyanka Chopra Jonas, etc., to name a few. In an analysis by Channel 4, it was found that there exists deepfake pornography of over 4000 celebrities all over the world on the internet.[6]

Another disturbing challenge that such AI-generated content poses before us is the creation of deepfake videos, which are further presented before the court of justice as evidence in a trial. A piece of information can be fabricated in a way that can build a particular case while not being genuine in the first place. The worst part is that such content can very easily be admissible in the court as evidence as they are very difficult to tell apart, if the right approach is not taken by using the correct algorithms to verify its legitimacy before admitting it. This was seen in a case that involved a fatal crash by a self-driving Tesla car where the plaintiff brought before the court a video where Elon Musk, the CEO of Tesla Motors, was seen vouching for the technological capabilities of Tesla cars, which his attorneys claimed could be a possible deepfake of Elon.[7] Instances like these could severely disturb the justice delivery mechanisms of various countries and lose people's confidence in them.

Along with the emergence of all the legal consequences, one of the major problems associated with the spreading of content like deepfake is that it makes the trust of the masses in the media and digital space for the dissemination of information very weak and makes it difficult for people to believe what they see on the internet. If places such as courtrooms are not safe from the evils of deepfakes, where such content can be used as an exhibit for evidence, it makes the trust of the masses in the state weak and vulnerable.

V. COMPARATIVE ANALYSIS OF GLOBAL LEGISLATIVE FRAMEWORKS

Currently, there is a global lack of legislation to regulate the production and circulation of deepfakes in all genres of media and entertainment. Since the technological advancement of

[6] N. Badshah, (2024). *Nearly 4,000 celebrities found to be victims of deepfake pornography* [Online]. The Guardian. Available at: https://www.theguardian.com/technology/2024/mar/21/celebrities-victims-of-deepfake-pornography (Accessed: 29 November 2024).

[7] Fortune. (2023). *Elon Musk's lawyers argue recordings of him touting Tesla Autopilot safety could be deepfakes*. Available at: https://fortune.com/2023/04/27/elon-musk-lawyers-argue-recordings-of-him-touting-tesla-autopilot-safety-could-be-deepfakes/ [Accessed 23 Nov. 2024].

deepfakes is a relatively newer concept that is still developing, though, at a great pace, it is difficult for the state to keep up with the legal policies and legislation regarding the same. More and more countries are updating their technology-related laws to counter this particular problem, one such example is China. It has brought in laws specifically to counter deepfakes and their illicit use. However, some countries still rely on their older laws and try to cover AI and deepfakes under the same ambit, for example, India, tries to incorporate the same under its Information Technology Act.

A more detailed study of the various forms of legislation brought with the objective of countering the illicit uses of deepfakes needs to be done to better understand the topic. The legislation of various major countries of the world is thus:

A. USA

There are two kinds of laws that are followed in the United States of America- federal and state laws. In terms of federal laws, there exists the No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of 2024 or the No AI FRAUD Act,[8] which prohibits and punishes the unauthorized usage and circulation of an individual's voice, likeness, etc., by an AI to generate deepfake or like the content. This is the primary legislation governing the usage of AI other than the supplemental legislations of copyright, defamation etc., according to the harm that is caused by the generation and dissemination of such content.

In terms of state laws, the states of California and Texas, to name a few, have led the forefront by bringing out relevant legislation to counter the problems created by deepfakes in the respective states. The laws for California (Assembly Bill 602[9] and Assembly Bill 730[10]) were implemented in the year 2019 itself. It particularly targets the prohibition of the usage of AI to create deepfakes for pornography and in election campaigns. The relevant law in Texas is titled *Unlawful Production Or Distribution Of Certain Sexually Explicit Videos,* which specifically intends to punish those using AI-generated deepfakes to run their political election campaigns.[11]

[8] H.R. 6943, 118th Cong. (2024).
[9] Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action, Assem. B. 602, 2019-2020 Reg. Sess. (Cal. 2020).
[10] Elections: Deceptive Audio or Visual Media, Assem. B. 730, 2019-2020 Reg. Sess. (Cal. 2020).
[11] Aled Owen: How Lawmakers are Tackling AI-Powered Manipulations, ONFIDO BLOG (Nov. 21, 2023), https://onfido.com/blog/deepfake-law/.

Although not a law in force at the time, there exists the COPIED Act (Content Origin Protection and Integrity from Edited and Deepfaked Media Act)[12], which is currently a bill aimed to protect the work of various kinds of artists such as singers, painters and journalists etc., from the evil hands of AI which is capable of making a similar artwork, so well detailed that the audience might fail to differentiate between the two. This is made with the intent to safeguard the rights of such aggrieved artists by attaching to each work a digital watermark, which would be called as 'content provenance information'. It has not become legislation yet but is a significant step in progress regarding the discussion and topic as it directly includes deepfakes of all sorts within its ambit and boundaries.

B. China

Regardless of its reputation as a country that is often criticized for human rights regarding personal freedoms, it is one of the first countries to bring out legislation to directly counter the production and usage of deepfakes inside the country. The legal provisions of the said law, which is the Deep Synthesis Provision, prohibit and punish the generation and usage of a deepfake of a person without their consent. It also mandates a disclaimer on deepfake content, which must say that it is generated with AI and is not real. It also puts a fair responsibility on media platforms to monitor and remove unauthorized deepfake content.[13] The law came into force in January, 2023. This law is a major step in the field because it incorporates within itself both the creator as well as the user of deepfake content.[14]

C. UK

Before the amendments brought to the Online Safety Act 2023[15], the kind of unauthorized content which is generated by means of AI utilizing mechanics of machine learning, such as deepfakes, was neither prohibited nor punished, as was the case established in various other countries. It also did not prohibit the circulation or dissemination of such content until and unless it could be proved by the aggrieved party that there was a clear intention to cause harm

[12] Content Origin Protection and Integrity from Edited and Deepfaked Media Act of 2024, S. 4674, 118th Cong. (2024).
[13] Ramluckan, T. (2024). *Deepfakes: The Legal Implications*. In Proceedings of the International Conference on Cyber Warfare and Security (ICCWS). Available at: https://doi.org/10.34190/iccws.19.1.2099 [Accessed 23 Nov. 2024].
[14] C. Briefing, (2022). *China to Regulate Deep Synthesis (Deepfake) Technology from 2023* [Online]. Available at: https://www.china-briefing.com/news/china-to-regulate-deep-synthesis-deep-fake-technology-starting-january-2023/ (Accessed: 2 December 2024).
[15] Online Safety Act 2023, c. 50 (U.K. 2023).

to them in the first place by such content. The prosecution had to establish, with the help of other kinds of laws present in the country, the kind of harm that had been done, such as defamation, fraud, harassment, etc. This, in turn, became very demanding for the prosecution to establish. The kind of approach taken by the United Kingdom in this regard was very opposite and, on the face of it, ridiculous, where a hypothetical person who is unauthorized deepfake pornography generated by AI is circulated on the internet had to prove the accused's intent to harm in order to get relief from the Court.

This was changed with the coming of the much-required amendments to the said Act, where the prosecution no longer has to establish the intent to harm the accused when such AI-generated explicit content is created and shared without the consent of the individual involved. It also now puts more stringent punishment on breachers of the said provisions of the law and explicitly puts deepfakes under its wide ambit. This is a giant step forward in by the lawmakers of the UK, which brought about the much-needed and required changes to the existing law of the land.

D. European Union

The European Union is subject to the first-ever comprehensive legislation with the objective of regulating the functioning and control of artificial intelligence in Europe. It is called the AI Act[16] and aims at harmoniously aligning the functioning of AI with the existing fundamental rights and ethical principles. Art 52(3)[17] of the Act mandates the creators of AI programs to create transparencies between the user and the AI and that the former must be made aware that it is being subjected to artificial intelligence. The DSA, or the Digital Services Act,[18] also runs on similar lines and provides provisions for increased transparency between the user and AI. This is helpful in providing disclaimers to users when they are subjected to content such as deepfake.[19]

[16] Artificial Intelligence Act, Regulation (EU) 2021/0236, 2021 O.J. (L 151) 1 (EU).
[17] Artificial Intelligence Act, Regulation (EU) 2021/0236, § 52(3), 2021 O.J. (L 151) 1 (EU).
[18] Digital Services Act, Regulation (EU) 2022/2065, 2022 O.J. (L 277) 1 (EU).
[19] AI-Generated Deepfakes: What Does the Law Say?, ROUSE (Jan. 2024), https://rouse.com/insights/news/2024/ai-generated-deepfakes-what-does-the-law-say.

VI. INDIAN LEGISLATIVE FRAMEWORK: CURRENT STATUS AND REGULATORY CHALLENGES

The legal provisions of India do not explicitly cover the harm that is caused by artificial intelligence at the present time. The remedy to damage done by such AI software can be brought under the wider ambit of other legislations such as the Bhartiya Nyaya Sanhita, 2023[20], to hold accountable various criminal offences committed through the use of AI liable under the primary penal law of India, and the Information Technology Act,2000,[21] which includes within itself various forms of cybercrimes, which can supplement the BNS to define the crimes committed with the help of technology of some kind.

For example, the creator of an unauthorized deepfake pornographic video of a woman being circulated in India can be held liable under the BNS in the following sections- Section 70 (Sexual Harassment), Section 356(1), and (2) for defamation, Section 351(4) for criminal intimidation and Section 79 for word, gesture or act intended to insult the modesty of a woman. Further, they would be liable under the following provisions of the Information Technology Act- Section 66E, which lays down punishment for capturing, publishing or transmitting an image that would construe a violation of privacy and Section 67 and 67A, which punishes an individual for transmitting obscene material in electronic form and materials containing sexually explicit acts.

There can be various kinds of deepfake content generated by Artificial Intelligence, which can attract different kinds of punishments from different legislations based on the type of damage that they intend to do. For example, a deepfake video of a terrorist organization that aims to bring unrest in the country and affect its integrity and sovereignty can attract Section 152 of BNS, and the creator can be held liable under threat to national security. Similarly, when someone's original work is swapped with another's data, such as audio or visual, the damage that it causes to the public is complemented by the copyright infringement issues that it attracts by the usage of such original work, following the Intellectual Property Laws of India, such as unlicensed use of original work.

[20] Bhartiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[21] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

Although, at present, India lacks particular legislation that specifically aims to counter AI-generated content such as deepfakes, it can be brought under the ambit of the new Act brought in by the government of India, which is titled **Digital Personal Data Protection Act, 2023.**[22] The Act has an objective of to strengthen protection against personal data which is digitally stored, the unauthorized use of which is the most important ingredient in the making and misusing of a deepfake content. It allows for the processing of only the data of an individual for which they have explicitly given their consent under Section 4 of the Act. Further, they can claim for correction or request for deletion of any unauthorized use of their private data under Section 12 of the Act. It also lays down punishments in Chapter VIII of the Act for those who breach the provisions of the Act.

VII. SOCIO-ETHICAL IMPLICATIONS AND TRUST PARADIGMS IN THE DIGITAL AGE

It is said that trust is the costliest thing in the world. It is so because trust and belief cannot be bought and purchased but earned and, at the same time, can also be lost if not maintained purely. Media, which is regarded as the fourth pillar of democracy, works on the trust of the people. It is called so because it ensures that its functioning is fundamentally free from the intervention of other parts of the government. People believe what they see and what is told to them, and this is the basic reason why media houses exist in every part of the world. However, with the kind of information reaching the masses through channels of social media and alike sources, people are getting aware of potential dissemination of false information. Misinformation spreads like wildfire in today's technological age. This has also led the masses to question the credibility of the major media houses of the nations. People are losing trust in what they see.

When the situation is so bad that an individual cannot differentiate between real and fake content that is put in front of them, it becomes the human tendency to raise doubts at the source providing that information in the first place. In today's world the fact that AI is capable of deceiving people with its generated content which is so similar to real is a smaller problem when we find that the entire structure of media and information circulation is at stake. A study conducted by Dr Sophie Nightingale from Lancaster University in the UK and Professor Hany Farid from the University of California, Berkeley, in the US, found that three faces rated most

[22] Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

trustworthy from a sample of 800 faces were synthetic faces while four most untrustworthy faces picked by the people were actual real faces.[23]

Other major aspects where such dissemination of misinformation can become big troublemakers are cases of national security and judicial evidences, which have been mentioned earlier in the paper. By usage of AI to produce deepfake videos of terrorist organizations to resurrect their leaders to spread message can cause global imbalance and terror. This can act as a source of movement of people and their minds. Even the presentation of fake evidences in courtrooms can shake the very core of the justice delivery system of nations around the world. It can leave major impact on democracies globally.

VIII. POLICY RECOMMENDATIONS AND LEGISLATIVE FRAMEWORK DEVELOPMENT

The technology behind deepfake, which is machine learning, is still very young. It is still developing and has reached only a tiny per cent of its possible attainable heights. It has already become a significant topic of discussion and invites a check on policies and regulations by the State to watch its functioning and prevent its misuse. The State must control the practice of making and publishing deepfakes through legislation to protect the more extensive interests of society. This must be done at the same pace that the technology is developing in order to keep up with the same. The more delayed the legislation becomes, the more difficult it will be for the laws and policies to keep up with technological advancements. The sort of data that AI has the potential to manipulate and produce into newer outputs is far beyond the limitations that humans can put. However, we must strive to overwatch its functioning to protect the fundamental rights of the citizens and ensure everyone has a life of dignity.

One of the most fundamental problems that arise when drafting legislation on matters such as AI and deepfake is to differentiate clearly as to who is to be held liable for the crime that is so committed with the help of AI. One line of argument can be drawn that since AI does not have a mind of its own, it relies on human intervention to provide an initial data set for further machine-based learning. This would hold the human controlling the AI initially liable for the offences that the AI commits, which can be based on the legal principle of vicarious liability.

[23] Sophie Nightingale & Hany Farid, AI-Synthesized Faces Are Indistinguishable from Real Faces and More Trustworthy, 119 PNAS e2120481119 (2022), https://doi.org/10.1073/pnas.2120481119.

On the contrary, it can be argued that after a point of time and subsequent development, it is the AI itself that controls its actions. Thus, it should very well suffer the consequences of such actions. Further in the latter case, it is to be determined as to how a punishment can be imposed on an AI. Can it be penalized to pay a fine or given the death penalty just like how humans are punished for their criminal wrongs?

In such cases, how to charge an AI for criminal offences also needs to be determined. The intention to commit a crime becomes a major deciding factor when adjudicating criminal cases, and the question that needs to be resolved is how can the intent of an AI be determined for the commission of a particular crime. If intent is impossible to determine, any person, be it natural or legal, could be set free of all charges. Thus, this stands as a major problem that needs to be tackled before forming legislation to charge AI with criminal offences. Even the legislation brought about by China to target deepfakes does not hold AI accountable; rather, it is the creator and user of the deepfake content who would be charged with offences.

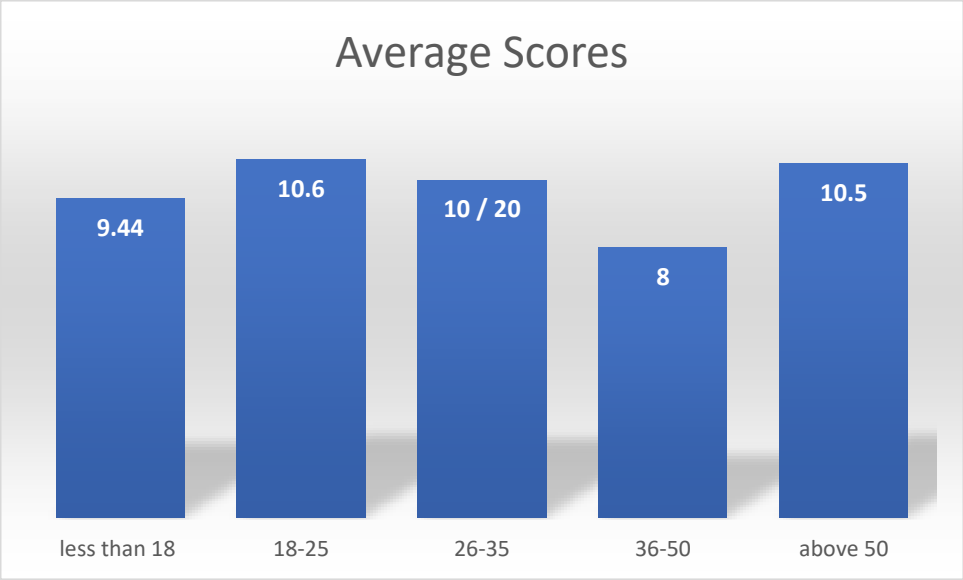
What also needs to be kept in mind is the kind of punishment that the legislation would aim to provide for. The very origin of deepfake was to provide a satirical source of entertainment before it took an evil turn of criminal consequences. Therefore, maintaining its original intent needs to be one of the primary foci of the legislation. This means that the use and generation of deepfakes, in general, must not be banned but only regulated strictly so as to curb their misuse while at the same time preserving their essence as a source of entertainment.

The most fundamental thing that must be considered is that the proposed legislation must align with the basic principles of the Constitution of India. Article 19(2) of the Constitution[24] enlists ‘defamation’ and ‘public morality’ as grounds for reasonable restriction on the fundamental right of freedom of speech and expression. This means that the proposed legislation shall have the backing of the principles of the constitution on the condition that the law should penalize only the deepfakes that are created with an intent to harm and proceed to defy the conditions listed in Article 19(2), which will then not be protected as a legitimated form of free speech and expression. This is mandatory so as to ensure that the law punishes only those who intend to work against societal interests. This perspective will protect the generation of deepfakes

[24] INDIA CONST. art. 19, cl. 2.

created with objectives such as education. The distinction between deepfakes used for entertainment with satirical illustrations must be differentiated from the unlicensed exploitative use of deepfakes.

Apart from legislation, what needs to be promoted the most by the State is awareness amongst the general masses. The hypothesis made before carrying out the research was that the age group of 18-25 years of age, which has been exposed to the most amount of technology and technological advancements in their growing ages, would be able to differentiate better between real and AI-generated deepfake as compared to those younger or older than them. This presumption was, however, proved wrong by the data collected by the research conducted in line with this paper, where a mixed bag of 20 images containing 10 pictures of each real and AI-generated picture was given to people of different age groups. The results proved the hypothesis wrong when similar scoring was found among the entire age groups with an average survey score of 10.42/20. The range of the scores was 6-15, and the Median of the scores was 10/20.



In conclusion, this research underscores the critical need for widespread awareness and education to combat the challenges posed by AI-generated deepfake images. The study initially hypothesized that individuals aged 18-25, having grown up alongside rapid technological advancements, would demonstrate a superior ability to differentiate between real and AI-generated images. However, the results contradicted this assumption, revealing consistent performance across all age groups. Regardless of age, participants achieved an average score

of 10.42/20, with a median of 10/20 and a score range of 6-15. These findings suggest that exposure to technology alone does not inherently improve one's ability to detect deepfakes.

This lack of variation in performance highlights the need for comprehensive educational initiatives that are inclusive of all age demographics. Rather than targeting specific groups, these programs should equip individuals with critical thinking skills and practical tools for identifying manipulated media. By integrating such training into school curricula, workplace programs, and public awareness campaigns, society can build resilience against the deceptive capabilities of advanced AI technologies.

Moreover, legislation alone is insufficient to address the widespread implications of deepfake technology. A multifaceted approach that includes education, robust legal frameworks, and technological safeguards is imperative. This study demonstrates that the problem transcends generational boundaries, emphasizing the need for collective action. By fostering a well-informed population capable of recognizing deepfakes, we can mitigate the risks associated with misinformation and digital deception, ensuring a safer and more trustworthy digital environment for all.

TECH AT THE TABLE: BRIDGING DIVIDES AND SETTLING SCORES IN MODERN ADR

— Karan Kataria[*]

ABSTRACT

The efficiency and effectiveness of the alternative dispute resolution (ADR) methods can be gauged by the increased and preferred use of ADR techniques over conventional dispute resolution mechanisms. Currently, ADR is not only used to resolve commercial disputes but also frequently addresses interstate disputes. The ADR mechanism eliminates the cost and time that are associated with the traditional court processes. Keeping in view the rapidly changing technological landscape globally in the 21st century, this paper attempts to investigate how technology can be used in ADR processes to transform capabilities by overcoming geographical barriers as highlighted and necessitated by the COVID-19 pandemic.

The paper also argues that incorporating technology-driven Alternative Dispute Resolution (ADR) into dispute resolution mechanisms raises a number of legal and ethical concerns that must be promptly addressed. Taking a step further, this paper advocates for the necessity of legislation to regulate the current technological void, particularly the relationship between artificial intelligence (AI) and dispute resolution mechanisms. This paper proposes a method for establishing accountability in cases of irrational or unjust AI-driven decisions so that fairness and reliability can be ensured and technology efficiency does not overlook human judgement but rather attempts to balance it. This work enables ADR to evolve into a more inclusive and effective dispute resolution mechanism in an increasingly digital world.

[*] The author is a Rajya Sabha Research Fellow and Lecturer at Jindal Global Law School, O.P. Jindal Global University (JGLS).

Keywords: Alternative Dispute Resolution, ODR, Technology, Ethical Responsibility

I. SETTING THE STAGE: THE EVOLUTION OF ADR IN THE DIGITAL ERA

Alternative Dispute Resolution (ADR) is a broad term for methods of resolving disputes that do not involve traditional legal processes. Arbitration, mediation, conciliation, and negotiation are some of the more informal and flexible methods of conflict resolution. ADR has gained global recognition for its ability to provide specialized solutions while maintaining confidentiality, making it especially appealing for commercial and international disputes. ADR has thus become indispensable for the timely resolution of cases with high-value considerations.[1]

The large number of commercial, civil, and international disputes necessitates efficient and timely dispute resolution mechanisms. Traditional litigation processes, while effective in providing equal opportunity to all parties and a high level of legal scrutiny, frequently experience significant delays, high costs, and procedural complexities. This is especially true in jurisdictions with backlogged judicial systems, where cases are decided after years of litigation.[2] ADR processes are shorter in duration, often taking months, making them more appealing and preferred option to parties seeking timely justice. Furthermore, because of its flexibility, ADR allows parties to choose expert arbitrators or mediators with subject-specific knowledge that can help improve the quality and appropriateness of their decisions.

In recent years, ADR has emerged as a versatile solution to commercial and civil disputes. Technology has always played a role in ADR; early adoption involved the use of tools such as email and case management software, while later adoption involved advanced technology such as AI contract drafting and research assistant. ADR Principles and Practice (1993), by authors such as Henry J. Brown and Arthur L. Marriott, provides a comprehensive historical overview of the rise of ADR and its integration with technology.[3] This foundational work is frequently cited in scholarly discussions about ADR's evolution and the incorporation of technology into dispute resolution processes.

[1] Gary Born, *International Commercial Arbitration* (3rd edn, Kluwer Law International 2021) 123-130.
[2] Marc Galanter, 'The Vanishing Trial: An Examination of Trials and Related Matters in Federal and State Courts' (2004) 1(2) *Journal of Empirical Legal Studies* 459, 470.
[3] *Henry J Brown and Arthur L Marriott, ADR Principles and Practice (2nd edn, Sweet & Maxwell 1993).*

Over the last few years, technology has redefined and modernized legal frameworks, particularly in the ADR process. The construction of digital tools has resulted in vastly different approaches to dispute resolution, ranging from electronic filing systems to fully online Online dispute resolution (ODR) platforms. The COVID-19 pandemic has accelerated the incorporation of technology into all legal processes, with courts, arbitration bodies, and mediation centers around the world switching to virtual platforms. Video conferencing, online case management systems, and even AI-powered tools have all helped to make ADR processing faster, more efficient, and less expensive. Technology certainly overcomes geographical distances and simplifies the process of managing cases; thus, it ensures that ADR does not become obsolete in this digital world.[4]

This paper discusses and analyses various technologies currently used in ADR, such as video conferencing, ODR platforms, AI, and blockchain, to determine how they affect the efficiency, transparency, and accessibility of dispute resolution processes. The paper will also look at ethical, legal, and regulatory issues related to the use of technology in ADR, providing a comprehensive understanding of both the opportunities and challenges that lie ahead for technology-driven ADR.

II. TRACING THE ROOTS: THE INTERSECTION OF ADR AND TECHNOLOGICAL EVOLUTION

ADR as a method of dispute resolution dates back to ancient civilizations. While a plethora of ADR methods that we witness today case in point being mediation, arbitration, and conciliation have long been used in dispute resolution in ancient Greece, China, and India. These methods of ADR were specifically valued and given more consideration because they possessed the ability to provide a timely, efficient and amicable solution to long-running disputes by primarily focusing on dialogue, negotiation, and mutual agreement.[5]Arbitration, for example, has been used in commercial disputes for centuries, with merchants turning to neutral third parties to resolve trade disagreements. Mediation and conciliation, too, evolved as nonbinding processes aimed at encouraging collaborative dispute resolution.[6]

[4] Susan Blake, Julie Browne and Stuart Sime, *A Practical Approach to Alternative Dispute Resolution* (6th edn, Oxford University Press 2020) 75-90.
[5] National Arbitration Forum, 'History of Alternative Dispute Resolution' (2021) https://www.adrforum.com/about/history-of-adr accessed 19 October 2024.
[6] William W. Park, *Arbitration of International Business Disputes: Studies in Law and Practice* (2nd edn, Oxford University Press 2012) 88-95.

The ODR began around the 1990s, when platforms like PayPal and eBay started deploying ODR to adjudicate disputes that involve lower-value claims and domestic disputes. Ethan Katsh and Janet Rifkin, in their seminal work "Online Dispute Resolution"*: Resolving Conflicts in Cyberspace'*[7] (2001), discuss the evolution and practical applications of ODR. Ethan Katsh in his later research for the *International Journal of Law and Information Technology*, expanded upon how AI and digital platforms can be harnessed for ODR. Further, Prof. Srikrishna Deva Rao, in his article *ODR: 'The Future of Dispute Resolution in India'*[8] (2020), analyses the potential of ODR in India particularly addressing the issue of the huge backlog of cases in India.

During the COVID-19 pandemic, the use of technology became a crucial part of the ADR process across the world, integration of technology in ADR was gradual before the pandemic, given that most of the practitioners relied on physical hearings and mediation sessions. There was an extraordinary shift towards fully virtual ecosystems for dispute resolution post-pandemic. Video conferencing tools like Zoom, Google Meet, online dispute resolution platforms, and AI-based case management systems became a necessity to ensure that the ADR processes are not affected by the COVID-19 lockdown.[9] They further promoted accessibility and efficiency during the pandemic. However, it is essential to discuss these tools in little detail before arguing for the ethical and legal accountability of ADR processes vis-a-vis technology.

III. TOOLS OF THE TRADE: EXPLORING TECHNOLOGIES TRANSFORMING ADR

Technology evolves and progresses in response to changing times. In today's world, technology began with simple emails in the last decade and has steadily moved towards virtual space with the help of video conferencing platforms, reducing or eliminating the need for physical presence and making it easy and accessible for parties. Video conferencing platforms such as Zoom, Microsoft Teams, and Google Meet have transformed the landscape of ADR by allowing parties in different locations to engage in real-time discussions without the need for physical presence. This is especially important in cross-border disputes where parties are

[7] *Ethan Katsh and Janet Rifkin, Online Dispute Resolution: Resolving Conflicts in Cyberspace (Jossey-Bass 2001).*
[8] *Srikrishna Deva Rao, 'ODR: The Future of Dispute Resolution in India' (2020) 3 NLUJ L Rev 45.*
[9] International Chamber of Commerce (ICC), 'History and Development of Arbitration' (ICC 2020) https://iccwbo.org/dispute-resolution-services/arbitration/ accessed 19 October 2024.

located in various jurisdictions.[10] It saves parties both in terms of time and travel costs, hence fastening resolution. Even the Supreme Court of India, in the case of State of Maharashtra v. Dr Praful B. Desai[11], echoed the argument that virtual methods can be used during arbitral proceedings to save time, which is the ultimate goal for which the court is attempting to incorporate such technology so that adjudication can be completed efficiently.

Moreover, in the virtual space, the breakout rooms for private discussions can be facilitated together with screen-sharing tools for the presentation of documents. This makes the ADR processes quite practical since interactions between the mediator, arbitrators, or other disputants are smooth. ICC report suggests that around 77% of international arbitrations made use of video conferencing during the COVID-19 pandemic.[12]

With rapidly changing technology, artificial intelligence is a new technological tool used to improve the efficiency of the ADR process. The emergence of AI has expedited the ADR process by offering capabilities such as data-driven insights, automation, and pattern recognition. The capabilities not only improve and streamline the procedural aspect of the ADR but also help in case management. Additionally, it aids in document analysis, legal research, and occasionally, even decision-making. Additionally, AI algorithms can be taught on past cases and given relevant, unbiased data and judgements to help them guess how a case might turn out. This means that these AI models can help arbitrators make better, more researched, and well-informed decisions. This utilization clearly demonstrates the deployment of these algorithms to provide insights into case outcomes.

While arguing that technological tools have helped the ADR process, it is essential that we also discuss how blockchains have introduced a new level of transparency in the ADR, especially arbitration. No record of agreement, contract, decision, or evidence can be altered; this is ensured by the decentralized, immutable ledger system that blockchain technology implements. It thus lends integrity to the dispute resolution process. Smart contracts, which are coded into the blockchain, are self-executing contracts that express the terms of an agreement in coded form.

[10] ICC, 'Videoconferencing in Arbitration: Best Practices and Challenges' (ICC 2021) https://iccwbo.org/resources-for-adr accessed 19 October 2024.
[11] (2003) Indlaw SC 320.
[12] International Chamber of Commerce (ICC), 'ICC Arbitration and COVID-19: A Survey of Videoconferencing Practices' (2021) *ICC Dispute Resolution Bulletin* 23, 25.

Lastly, the recent use of digital authentication tools and e-signatures improves the trust and reliability of technology in dispute resolution mechanisms. This approach uses technology to improve technology-aided alternative dispute resolution mechanisms. There are several reasons why the use of e-signatures and electronic authentication, especially when parties are located in different jurisdictions, facilitates easy flow through the ADR process: documents are signed digitally, securely, lawfully, free from tasks associated with paper, long and often cumbersome processes, and other burdens associated with the same. Built-in encryption and authentication systems with tools such as DocuSign ensure that signed documents remain confidential and tamper-proof.[13]

The practice of e-signatures, apart from saving time and resources, also provides confidentiality in the ADR process by securing sensitive agreements and merely letting authorized parties access them for signing. Technologically, this innovation even makes it possible to achieve a global reach in ADR processes. Parties from different countries can sign and authenticate their agreements as soon as possible.

IV. NAVIGATING ETHICS: CHALLENGES OF AI IN ADR SYSTEMS

The increasing dependency on Artificial Intelligence in Alternative Dispute Resolution raises various critical questions on fairness, bias, and transparency. The ADR system usually relies on historical datasets in training predictive algorithms or AI-driven mediators that inherently reflect any societal bias. An example is when a study conducted by the European Union Agency for Fundamental Rights pointed out how AI algorithms may perpetuate discriminatory practices when the situations involved relate to socio-economic or racial factors.[14] Again, the fairness of decisions rendered through AI in ADR would be called into question because the datasets on which the algorithms depend may not fairly represent diverse or marginalized populations.

Moreover, AI systems increase the opaqueness of decision-making that raise ethical issues. A great majority of AI models, especially most machine learning algorithms, act like "black boxes" whereby even their creators do not clearly understand how decisions are made. Such

[13] David A. Sorkin, 'Digital Signatures and Authentication in ADR: A Comparative Analysis' (2021) 12(3) *Dispute Resolution Journal* 64, 67.

[14] European Union Agency for Fundamental Rights, 'Data Quality and Algorithmic Bias: Addressing Discrimination in AI' (2020) https://fra.europa.eu/en/publication/2020/ai-discrimination accessed 20 October 2024.

obscurity is inconsistent with fairness and justice, the cornerstones of ADR.[15] The Ethics Guidelines for Trustworthy AI of the European Commission outlines requirements for transparency as a factor in ensuring trust in AI-driven decision-making processes. In the context of ADR, if parties cannot understand how the AI system ended up with a specific decision, it may undermine their confidence in the legitimacy of the outcome. Thus, stricter ethical regulation is called for concerning the use of AI-driven systems in ADR so as not to malign those very important pillars of neutrality, equality, and equity.

The internet-based version of Alternative Dispute Resolution (ADR), or Online Dispute Resolution (ODR), leverages technology to settle disputes outside the boundaries of the conventional judicial mechanism. The advent of Artificial Intelligence (AI) has greatly enhanced ODR, making it more accessible, cost-effective, and streamlined. AI-driven ODR deploys a blend of technologies, including Natural Language Processing (NLP), automated negotiation, and predictive analytics, to eliminate and automate the mechanisms of settling disputes. These technologies assist in categorizing disputes, legal argument analysis, and proposing settlements based on previous experience. The increased use of AI for legal decision-making is a step towards a digital justice system aimed at providing decreased court backlogs and better access to justice.[16]

AI is transforming ODR through automation of the essential aspects of dispute resolution. Computerized case management systems sort out disputes and suggest resolution pathways, minimizing administrative inconvenience. Artificial intelligence-powered tools such as virtual mediators and chatbots skillfully guide parties through the negotiation process through evidence-based practices. Predictive analysis reviews history to predict likely case outcomes, allowing parties to make more informed decisions. Meanwhile, natural language processing enhances document analysis, thereby improving consistency and accuracy in legal reasoning. Blockchain-activated smart contracts further enhance ODR by facilitating the automatic enforcement of agreements, with compliance assured without the intervention of the courts.[17] All of these innovations make ODR considerably easier in international business and e-

[15] European Commission, 'Ethics Guidelines for Trustworthy AI' (2019) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419 accessed 20 October 2024
[16] Davide Carneiro et al., *Online Dispute Resolution: An Artificial Intelligence Perspective,* 38 Artif. Intell. Rev. 1 (2012).
[17] Hibah Alessa, *The Role of Artificial Intelligence in Online Dispute Resolution: A Brief and Critical Overview*, 31 Info. & Common's Tech. L. 1 (2022).

business, where disputes usually involve remotely situated parties and relatively low-value monetary claims.[18]

The use of AI in ODR has various benefits and speeds up conflict resolution through the elimination of redundant work, delays, and general inefficiency. Cost savings are also an added benefit because AI-based systems minimize the use of legal practitioners, thus curbing the amount of money spent on conflict resolution. Scalability and accessibility are also increased, allowing individuals in underserved and rural communities to access digital means to resolve conflicts. In addition, AI promotes uniformity in the decision-making process through the application of uniform legal principles, eliminating human frailties and biases.[19]The use of the application of ODR has increasingly been adopted because it can maintain the informality of ADR while using AI to improve procedural efficiency.[20]

Despite these advantages, AI-based ODR systems have some disadvantages. One of the main disadvantages is the possibility of AI algorithm bias since machine learning algorithms that learn from past data may inherit past bias, leading to biased outcomes. Additionally, AI-based decision-making is a "black box," and it is difficult to explain or appeal the rationale for certain resolutions.[21] Legal accountability is another burning question. If an AI system makes an unjust decision, nobody knows whom to hold accountable. In addition, there are privacy and data security concerns since AI-based ODR systems process sensitive legal and personal information, necessitating robust cybersecurity. AI also makes it difficult to consider important human factors, like emotional responses and intangible considerations, that influence negotiations, which play an important role in cases involving personal relationships, like family law cases.[22] AI can optimize efficiency, but justice is often regarded as essentially human excellence, and substituting human judges with AI entirely is, therefore, an ethically complex question.[23]

Against this backdrop of issues, a regulatory framework needs to be established to make AI-based ODR fair, transparent, and accountable. Human supervision of AI-driven decisions needs to be firmly established to build trust in the justice system. Periodic audits of AI and rigorous

[18] E. Wilson-Evered & John Zeleznikow, *Artificial Intelligence and Online Family Dispute Resolution* (2021).
[19] Carneiro et al., supra note 1.
[20] Temitayo Bello, *Online Dispute Resolution Algorithm; Artificial Intelligence Model as a Pinnacle* (2017).
[21] Alessa, supra note 2.
[22] Id.
[23] Wilson-Evered & Zeleznikow, supra note 3.

bias testing need to be conducted to reveal and remove systemic defects before deployment. Legal and ethical measures need to be put in place to regulate AI in the resolution of conflicts to ensure due process and that inherent human rights are not undermined. Furthermore, AI needs to be integrated into judicial infrastructures, such as India's e-Courts system, to create a hybrid model where AI supports but does not substitute human adjudicators.[24]

AI can revolutionize dispute resolution, but its use must be supported by ethical standards and regulatory oversight. A harmonised strategy, where AI augments human judgement and not replaces it, looks at technology development employed as a tool for justice and not as a tool for legal expertise. With AI designing the future of ODR, fairness, transparency, and accountability will be of the utmost importance in ensuring its position in legal decision-making.

V. LEGAL ACCOUNTABILITY FOR DECISIONS MADE BY AI SYSTEMS

Perhaps one of the most contentious legal issues regarding AI in ADR is the accountability for decisions derived through such systems. Unlike their human peers, arbitrators or mediators being held personally liable for such decisions, an AI system cannot be viewed with regard to the same kind of accountability. If the AI-driven ADR system involved causes an unfair or inappropriate outcome, it is vague under the existing law who might be held liable: the people developing the AI, those designing the arbitration, or the parties using the system.

Currently, there is no clear opinion regarding the assignment of the burden of legal liability in ADR systems driven by AI. Some jurisdictions will hold liable the developers of the AI for defects in the algorithm itself, whereas in some others, there will be legal responsibility laid on the party that chose to integrate the AI system into the dispute resolution process. The European Parliamentary Research Service has issued a briefing note pointing out the lack of clarity on legal liability imposed on artificial intelligence systems in many areas, including Alternative Dispute Resolution. Such uncertainty is highly disturbing in high-stakes disputes, such as international commercial arbitration, where an incorrect judgment may have huge financial ramifications.[25]

[24] Carneiro et al., supra note 1.
[25] European Parliamentary Research Service, 'Artificial Intelligence and Civil Liability' (2020) PE 642.839 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)642839 accessed 20 October 2024.

To bridge this gap, the concept of setting independent regulatory frameworks specifically for AI in ADR. The Council of Europe has proposed the use of a legal scheme where it grants parties the right to appeal decisions made by AI systems in case bias or mistakes are suspected. Until such regulatory frameworks are designed and implemented generally across all jurisdictions, issues regarding the legality of AI-assisted decisions in ADR remain uncertain.

The Council of Europe (CoE) has established a comprehensive framework to ensure that artificial intelligence (AI) development aligns with fundamental human rights, democracy, and the rule of law. This framework encompasses principles such as respect for human dignity and individual autonomy, transparency and oversight, accountability and responsibility, equality and non-discrimination, privacy and data protection, and promoting reliability, safety, and trust in AI systems. For instance, the CoE's *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems* emphasizes these principles to guide ethical AI integration in the judiciary.[26]

In the Indian context, adapting these principles requires a nuanced approach that considers the nation's unique socio-legal landscape. Respecting human dignity and individual autonomy can be reinforced by ensuring AI applications do not infringe upon constitutional rights, aligning with Article 21 of the Indian Constitution, which guarantees the right to life and personal liberty.[27] Enhancing transparency and oversight could involve mandating that AI-driven decisions, especially in public services, are explainable and subject to human review, thereby fostering public trust. Establishing clear accountability mechanisms is crucial; for example, in the judiciary, reliance on AI for legal research has led to concerns about the generation of fake case citations, as highlighted by Justice Gavai.[28] Ensuring equality and non-discrimination necessitates that AI systems undergo rigorous audits to prevent biases, thereby upholding the constitutional mandate for equality before the law.[29]

Protecting privacy and data is a critical aspect of AI governance in India. The Supreme Court, in *K.S. Puttaswamy v. Union of India*, recognized the right to privacy as a fundamental right

[26] *Council of Europe - European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment, COE* (2018), https://coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment.
[27] INDIA CONST. art. 21.
[28] *Relying on AI for Legal Research Risky; Platforms Like ChatGPT Have Generated Fake Case Citations: Justice Gavai, LiveLaw* (Feb. 2025), https://www.livelaw.in/top-stories/relying-on-ai-for-legal-research-risky-platforms-like-chatgpt-have-generated-fake-case-citations-justice-gavai-286190
[29] *AI Watch: Global Regulatory Tracker - Council of Europe, White & Case (May 13, 2024),* https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-council-europe

under Article 21 of the Constitution.[30] This judgment establishes the legal foundation for regulating AI systems that process personal data, necessitating compliance with India's *Digital Personal Data Protection Act, 2023*.[31] Additionally, promoting reliability, safety, and trust in AI requires setting national standards for AI development and deployment, ensuring these systems are robust and secure.[32]

Legally, India can strengthen its AI governance by integrating these principles into existing frameworks. Amending the *Information Technology Act 2000* to include explicit provisions on AI ethics and accountability can provide a legal backbone for responsible AI use.[33]Incorporating guidelines for AI deployment in arbitration and dispute resolution processes can enhance the efficacy of the *Arbitration and Conciliation Act of 1996*.[34]Additionally, aligning AI practices with data protection regulations is essential, especially in light of recent legal challenges, such as the copyright lawsuit filed against OpenAI by global publishers in India, which underscores the need for clear legal guidelines on AI's use of copyrighted material.[35] By embedding these principles into its legal and policy frameworks, India can harness AI's benefits while safeguarding individual rights and societal values.

VI. BALANCING HUMAN DISCRETION WITH TECHNOLOGY-BASED DECISIONS

The use of technology certainly does not lead to an end of human discretion, especially in disputes having complexity and requiring substantial emotional intelligence, empathy, and cultural sensitivity. That cannot easily and perfectly be reeled out by human mediators or arbitrators as 'gut instinct' and 'judgment' qualify them, which are often impossible to mirror in an AI system. Often, in family disputes and sensitive issues involving culture, solutions had to be found by ensuring that they were not only determined from a law standpoint but also to make sure that members of the parties were better understanding each other.

[30] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.
[31] *The Digital Personal Data Protection Act, 2023*, No. 30, Acts of Parliament, 2023 (India)
[32]*Navigating Challenges with AI-Enhanced Online Dispute Resolution*, IndiaAI (Feb. 2025), https://indiaai.gov.in/article/navigating-challenges-with-ai-enhanced-online-dispute-resolution (last visited Mar. 13, 2025).
[33] *Information Technology Act*, No. 21 of 2000, Acts of Parliament, 2000 (India).
[34] *Arbitration and Conciliation Act*, No. 26 of 1996, Acts of Parliament, 1996 (India).
[35] Aditya Kalra, *OpenAI Faces New Copyright Case from Global Publishers in India*, Reuters (Jan. 24, 2025), https://www.reuters.com/technology/artificial-intelligence/openai-faces-new-copyright-case-global-publishers-india-2025-01-24/

There has to be a fine balance between human intervention and technology support. Even though good for the usual management of cases, analysis of data, and even initial evaluations in the case, AI should reserve wide decision-making authority to human arbitrators or mediators in complex, controversial matters. "AI can support but may not replace human discretion," according to a report from the Program on Negotiation at Harvard Law School. The report further finds that, while AI might appear to deliver data-driven insights, it is far inferior in human-behavioural nuances, emotions, or cultural context dictates, which often prove decisive in dispute outcomes.

Moreover, over-reliance in ADR on AI will further reduce human discretion and judgment. The legal scholars warn that where the AI systems are regarded as the primary decision-makers, the human actors are most likely to become facilitators who are passive toward the recommendations of the AI. This would downsize the active role of mediators and arbitrators explaining the law and considering a broader socio-legal context of dispute. That would mean preserving a hybrid approach where AI enhances human capabilities without fully displacing human elements in ADR.[36]

VII. INTEGRATION OF VIRTUAL REALITY (VR) IN MEDIATION AND ARBITRATION

With Virtual Reality technology, the entire ADR landscape is to change because the experiences it will be offering are really immersive, and that should translate into better understanding and involvement in mediation and arbitration procedures. The use of VR in ADR presents an unprecedented opportunity for stakeholders to encounter scenarios under controlled circumstances that should prompt empathy and facilitate resolving issues involved.[37] According to the International Institute for Conflict Prevention & Resolution, also known as CPR, immersive VR environments may mimic real-world conditions. Participants could thus understand one another and their drivers much better. Such an ability can be crucial when conflicts feature complex emotional and psychological factors.

[36] Council of Europe, 'Artificial Intelligence and Human Rights: Challenges and Recommendations' (2021) https://www.coe.int/en/web/artificial-intelligence accessed 20 October 2024.
[37] International Institute for Conflict Prevention & Resolution, *Virtual Reality in Conflict Resolution: The Future of Mediation and Arbitration* (2019), https://www.cpradr.org/.

Apart from that, VR can bridge geographical gaps. That is, the parties on either side can interact face-to-face without necessarily attending the same venue. That is, it allows easier access and is cost-effective as regards dispute resolution. For instance, the Oman Chamber of Commerce and Industry recently started using VR technology in its dispute resolution proceedings where participants would socialize in a virtual space that bears a similarity to a real courtroom.[38] Overall, the prospect of VR in ADR seems very promising, but there are indeed very significant challenges concerning the accessibility of the technology, requirements for specialized equipment, and training in proper use.

A. Expansion of Blockchain-Based Contracts and Dispute Resolution

Blockchain technology may revolutionize the ADR process by providing secure, transparent, and tamper-proof environments for managing contracts and resolving disputes. Automating the execution of agreements through blockchain-based smart contracts ensures their fulfilment on agreed terms without any need for intermediaries.[39] Smart contracts reduce time and costs associated with traditional forms of dispute resolution according to the World Economic Forum report. This is owing to the fact that smart contracts can provide clear, immutable records of every single transaction and interaction.

Furthermore, blockchain can support decentralized dispute settlement mechanisms, whereby parties are able to settle disputes away from the central authority. Not only will it increase accessibility but also ensure fairness and transparency within the framework of the dispute resolution system.

However, the widespread adoption of ADR on blockchain still faces several hurdles, primarily regulatory uncertainties and problems that require standardization in the way that disputes are resolved on blockchain platforms. As governments and institutions understand the potential of blockchain for ADR, creating such comprehensive legal frameworks will be crucial in facilitating innovation without protection for all parties involved.[40]

---

[38] Oman Chamber of Commerce and Industry, *Innovations in Dispute Resolution: The Use of Virtual Reality in Arbitration Proceedings* (2022), https://www.chamber.org.om/.
[39] World Economic Forum, *Blockchain Beyond the Hype: A Practical Framework for Business Leaders* (2020), https://www.weforum.org/reports/blockchain-beyond-the-hype.
[40] European Union Agency for Fundamental Rights, *Blockchain and Smart Contracts: An Overview* (2021), https://fra.europa.eu/en/publication/2021/blockchain-and-smart-contracts-overview.

B. Role of 5G in Enabling Faster, Global ADR Proceedings

Admittedly, the introduction of 5G technology has promised to increase the efficiency and effectiveness of ADR through greater speed and reliability of communication. 5G technology drastically increased data transmission rates and reduced latency-is well set to accommodate instantaneous collaboration among parties, arbitrators, and mediators from all over the world. For online dispute resolution, in particular, the exchange of information must be prompt in the resolution of disputes.

However, the Adoption of 5G technology may vary in different regions. Developing economies may face various challenges when trying to upgrade their telecommunication infrastructure to support 5G, which means their access to ADR technologies may see an increased digital divide. Therefore, the policymakers have to work on those disparities so that all parties can benefit from advancements in communication technology.[41]

VIII. CLOSING THE LOOP: TOWARDS A TECH-DRIVEN AND EQUITABLE FUTURE IN ADR

The integration of technology into Alternative Dispute Resolution (ADR) processes is a crucial step in conflict resolution practices. This study looked into several aspects of this shift, such as the historical context, different types of technologies, the benefits, challenges, and emerging trends. However, the study reflects a significant number of challenges, which must be addressed during the course. Video conferencing technologies, ODR frameworks, and artificial intelligence-based applications have made the concept of dispute resolution more accessible, particularly to people living in remote areas or developing economies. For example, India: The implementation of ODR platforms demonstrated how technology can make the process less burdensome for parties. Furthermore, the expansion of blockchain into new areas allows for greater transparency and trust within contracts, as well as predictive analytics that allow for informed decision-making when resolving disputes.

The digital divide is vast and is currently exacerbated, particularly in developing economies, where barriers to equitable use of technology in ADR remain significant at times. Cybersecurity concerns, as well as the ethical implications of AI, have created complexities

[41] Chen, T. & Jiang, C., *5G and Its Role in the Future of Dispute Resolution: An Exploration* (2021) 26 Harvard Negotiation Law Review 243, https://doi.org/10.2139/ssrn.3638348.

that must be handled carefully in order to ensure fairness and accountability in conflict resolution processes. Because technological change contributes to legal change, the legal frameworks that govern ADR must also change in order to address new changes that arise as a result of it.

Policymakers must focus on developing comprehensive legal frameworks that specifically address the use of technology in dispute resolution; these frameworks should detail accountability, ethical considerations, and standards for the application of technology, such as AI and blockchain.

Second, efforts to bridge the digital divide must include investments in infrastructure and training, particularly in developing economies. Governments, non-governmental organisations (NGOs), and international organisations must pool their efforts, resources, and expertise to ensure that technology in ADR is accessible to all, including disputing parties.

Whereas on the other side, the ongoing deliberations among the stakeholders that include not only industry but also lawyers and academia, who are critical of catching up with the fast-moving and ever-evolving technology advancements. In order to comprehend the impact and implications of evolving technologies on ADR processes, all the stakeholders must collaborate with technologists. This will result in innovative solutions and acknowledging the law and ethics.

As a result, while technology offers unprecedented opportunities to improve ADR processes, it must be approached with caution due to ethical, legal, and practical implications. By addressing these challenges through collaborative efforts and well-defined regulatory frameworks, the ADR landscape can evolve into a more accessible, efficient, and just system for resolving disputes in the digital age.

INDIA'S WAY TO MANAGE AI: AN ALTERNATE TO SPECIFIC REGULATION?

— *Aishwarya Gautam*[*]

ABSTRACT

In the digital age, technologies have become essential for functioning efficiently and adhering to the digital globe. One of such technologies is Artificial Intelligence. AI has become a prominent part of daily life. Along with its efficiency, AI constitutes opaque and shadows the fairness in the procedure of its functioning. It is not ethically and legally correct. To outcast this concern, many countries have implemented laws to manage AI-associated issues, but India is lagging behind in the race. The country is awaiting the full exploration of the potential of AI before drafting a bill to coup AI in the country. With India's infrastructure and reliance on AI, the country is behind in making laws. It is costing the country with compromised access to the technologies. However, with the growing paced development of technology and economy, as well as the advancement of society, AI has entered into the realm of every industry in India. It has become essential for these industries to make AI functional in affirmation to delete drawbacks of it in the work. Keeping this view in their mind, they have chosen to issue guidelines themselves as waiting for a centralised effort to bring legislation may, till then, cause havoc. Since AI is a complex technology, it is essential for the law-maker to build a law quickly rather than waiting for an opportunity to occur. This waiting period has its own costs, from privacy infringement to financial injury, therefore making AI unreliable for local usage. It will be beneficial for the country to bring a specific regulation for AI quickly.

[*] The author is pursuing LL.M. (Technology & Law) from Hidayatullah National Law University, Raipur (HNLU).

I. INTRODUCTION

In the age of emerging technologies, reaching and laying back on generative automated technologies to make critical decisions has become easier. The vision of deployment of technologies like artificial intelligence (AI), among others, is being manifested in many sectors today across India and around the globe. There is no doubt that the usage of AI, for example, in healthcare and the legal profession in recommending over-the-counter medicines and smart contracts, etc., has become prominent in easing the baseline tasks of professionals. Along with this, AI has made administrative tasks efficient and diverted human resources where it is required to be present the most. Other sectors like education, meteorology, and banking are also finding ways to install customised AI to fulfil their needs and demands. Its significance has been strengthened in today's digital realm.

AI gained popularity in the current decade since the drastic usage of ChatGPT, but Alan Turning defined AI back in the 1950s as the "ability of computer programs to mimic human responses."[1] His approach showed AI is controlled in three elements, one by the computer itself and the other two by human beings. The elements reflect AI's potential to mimic intelligence in replicating human intelligence. What has been noted is that Machine Learning (ML) learns and mimics human intelligence by feeding previous strategies and responses developed by human beings. Such a method is known as 'data mining'. With this, it can be understood that AI has the potential to learn, adapt, sense, and respond as per the strategy of data mining. The following components of AI are learning, reasoning, problem-solving, perception, and language-understanding.[2]

But the birth of AI can be traced back to older times than the 'turning test.' A workshop organised by John McCarthy in 1956 at the Dartmouth Summer Research Project on Artificial Intelligence showcasing his idea of stimulating intelligence in machines.[3] All of the later references in that millennia related to AI went back to McCarthy.

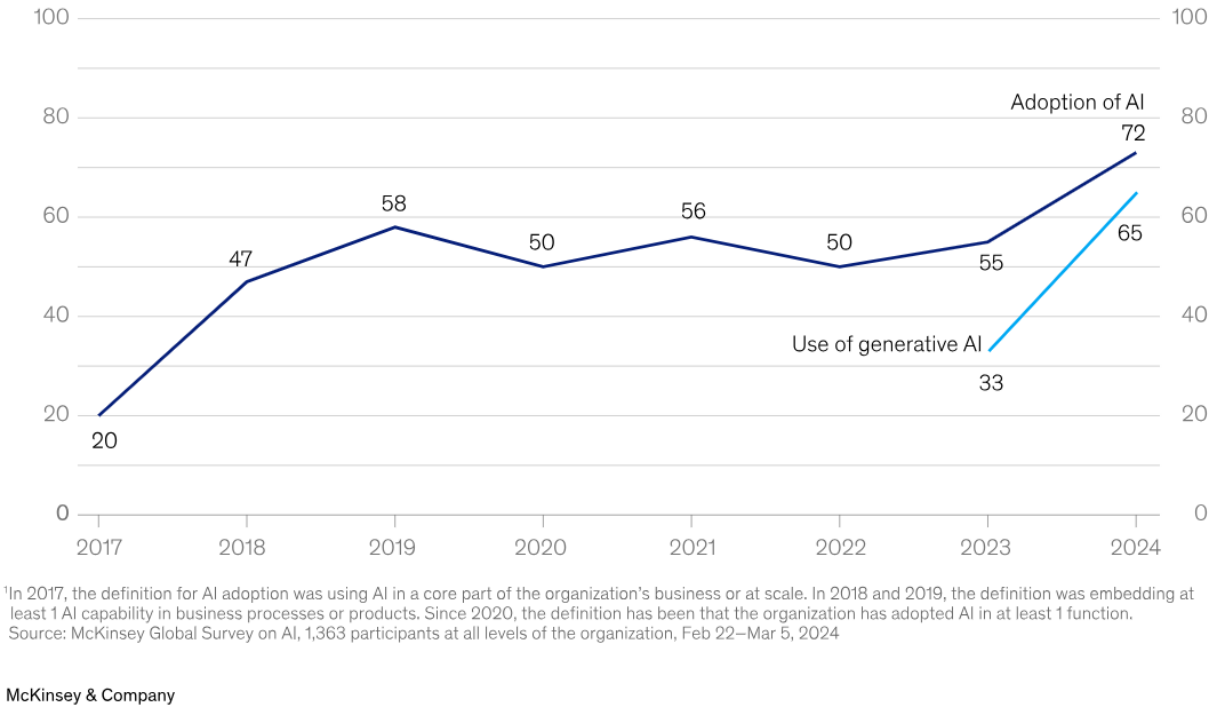
---

[1] Stephen Muggleton, 'Alan Turing and the development of Artificial Intelligence' (2014) 27(1) AI Communications https://www.doc.ic.ac.uk/~shm/Papers/TuringAI_1.pdf accessed 02 January 2025

[2] Ibid.

[3] Michael L. Littman, Ifeoma Ajunwa, Guy Berger, Craig Boutilier, Morgan Currie, Finale Doshi-Velez, Gillian Hadfield, Michael C. Horowitz, Charles Isbell, Hiroaki Kitano, Karen Levy, Terah Lyons, Melanie Mitchell, Julie Shah, Steven Sloman, Shannon Vallor, and Toby Walsh. 'Gathering Strength, Gathering Storms: The One Hundred Year Study on Artificial Intelligence (AI100) 2016 Study Panel Report.' (2016) One Hundred Year Study on Artificial Intelligence, Stanford University, Stanford, CA https://ai100.stanford.edu/2016-report/appendix-i-short-history-

In India, AI was first brought to the country by Professor H.N. Mahabala in the 1960s in one of the leading institutes in the country, IIT Kanpur, to help in research and academia at the university.[4] Since then, AI has been adopted in a managerial way across the country rapidly, as shown in the graph below.[5]



[1]In 2017, the definition for AI adoption was using AI in a core part of the organization's business or at scale. In 2018 and 2019, the definition was embedding at least 1 AI capability in business processes or products. Since 2020, the definition has been that the organization has adopted AI in at least 1 function.
Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

The figure represents the adoption of AI in businesses across the globe in at least one or more deliveries of functions, pointing towards the demanding usage of AI in various industries around the globe. Keeping this in mind, a few countries (USA, European Union, South Korea, Canada, etc.) have implemented laws related recently to manage threats, especially to manage high risks. Despite its benefits, difficulties emerging from AI outweigh the positive approach of using it. With this note, as of today, there is no formal statute to regulate AI in India, and it may cause havoc if no such sustainable step is taken in the near future. No doubt, the government is trying to bring regulations and guidelines in bits (discussed in 4.0), but that may

ai#:~:text=The%20field%20of%20Artificial%20Intelligence,solving%20a%20system%20of%20equations. Accessed 31 December 2024

[4] Anirban Sen and T V Mahalingam, 'Meet Professor HN Mahabala, the man who mentored India's IT icons' *The Economic Times* (Bengaluru, 23 July 2016) https://economictimes.indiatimes.com/tech/ites/meet-professor-hn-mahabala-the-man-who-mentored-indias-it-icons/articleshow/53346662.cms?from=mdr accessed 31 December 2024

[5] Alex Singla, Alexander Sukharevsky, Lareina Yee, and Michael Chui, and Bryce Hall, 'The state of AI in early 2024: Gen AI adoption spikes and starts to generate value' (*QuantumBlack AI by McKinsey*, 2024) https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai accessed 03 January 2024

not have been proven to be the best. In spite of whatever steps are taken to manage AI in usage correctly, infringement of rights and duties exists in the corner.

II. WHAT IS IN FOR AI IN INDIA

India is the most populous country in the world, with over 936 million internet users, as revealed by the Telecom Authority of India,[6] making the country the second biggest user of its facilities. There is no denying the country's potential to take the first spot, as most of the chores in the country have shifted into the decorum of digitalisation. The young generation of the country is heavily relying on the Internet to get work done- be it for academics, work or leisure. Systematic development and shifting towards digitalisation of the payment system by introducing Unified Payment Interference, locally known as UPI, is one of the significant showcases of the country's vision of Digital India.

Benefits have not been limited to residents of the country but to almost all of the sectors thriving and flourishing in the country. Banking and financial services use AI to provide better customer experience at the comfort of distance, avoiding the hassle of waiting and waiting hours. Specific AI learns and provides a seamless interface of personal accounts like transactions and auto-generated bank statements, suggesting the best scheme and its potential outcomes specifically customised to the customers and solving queries using chatbot assistance. Apex bank, Reserve Bank of India, using the technology to trace digital frauds.[7] Another major sector, railways, has also deployed AI to provide platforms for users to produce on-demand electronic tickets, guide trains' running schedules, and provide platform information on the basis of previous patterns.[8] Online shopping sites recommend users' products based on personalised choices based on previous search history, creating customised experiences. It even determines the type of style that will suit someone based on their body mass index.[9] Digital

[6] Tech Desk, 'India crossed 936 million internet subscriptions in December 2023: TRAI' *The Indian Express* (India, 24 April 2024) https://timesofindia.indiatimes.com/technology/tech-news/india-now-has-936-16-million-internet-subscribers-trai/articleshow/109537789.cms accessed 01 January 2025

[7] Sunainaa Chadha, 'Explained: RBI is using an AI tool MuleHunter.ai to cut down digital frauds' *Business Standard* (Mumbai, 09 December 2024) https://www.business-standard.com/finance/personal-finance/explained-rbi-has-a-new-ai-tool-mulehunter-ai-to-reduce-digital-frauds-124120900250_1.html accessed 01 January 2025

[8] Twesh Mishra and Surabhi Agarwal, 'Railways taps AI to improve seat availability on high-demand routes' *The Economic Times* (India, 17 October 2024) https://economictimes.indiatimes.com/tech/technology/railways-taps-ai-to-improve-seat-availability-on-high-demand-routes/articleshow/114292716.cms?from=mdr accessed 02 January 2025

[9] Erik Lindecrantz, Madeleine Tjon Pian Gi, and Stefano Zerbi, 'Personalizing the customer experience: Driving differentiation in retail' (*McKinsey &Company*, 28 April 2020) https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail accessed 02 January 2025

health applications also employ AI, which determines specific medicines based on patient's health information or by uploading prescriptions online. It also can generate daily routines and reminders for the betterment of its users. Judicial stakeholders are also using 'legal predictive models' to generate potential outcomes based on similar previous facts and circumstances, and decisions.[10] Usage of Alexa, Siri, etc, is widely prevalent, and therefore, the list can go on.

Despite a massive reliance on AI, India has no specific laws for AI. It is a good thing that the concept of 'autonomy' exists in the democratic setup of the country. Security Exchange Boards of India (SEBI) issued a monumental step to strengthen standards of data privacy, ensuring transparency in AI operations and accepting entire operational liability for AI-generated outcomes.[11] The Honourable Supreme Court of India has banked the usage of AI in August 2024 for legal research, judgment translation[12], and AI Saransh for generating summaries of pleadings[13]. The Indian Council of Medical Research has issued "Ethical guidelines for the application of Artificial Intelligence in Biomedical Research and Healthcare" to ensure the autonomy of patients' consent, non-maleficence, data governance, risk-mitigation strategies against data breaches, etc. In this strategic way, entities have to deal with AI-related concerns on their own.[14]

The real issue that still lingers despite efforts of institutions, bodies, or organisations, be it private or public, is the lack of centralised legislation to deal with AI-related risk management.

---

[10] Sugam Sharma, Ritu Shandilya, and Swadesh Sharma, 'Predicting Indian Supreme Court Decisions' (2021) SSRN Electronic Journal https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3917603 accessed 02 January 2025

[11] SEBI, 'Proposed amendments with respect to assigning responsibility for the use of artificial intelligence tools by Market Infrastructure Institutions, Registered Intermediaries and other persons regulated by SEBI' (November 2024) https://www.sebi.gov.in/reports-and-statistics/reports/nov-2024/proposed-amendments-with-respect-to-assigning-responsibility-for-the-use-of-artificial-intelligence-tools-by-market-infrastructure-institutions-registered-intermediaries-and-other-persons-regulated-b-_88470.html accessed 02 January 2025

[12] The Hindu Bureau, 'Supreme Court confirms use of AI in legal research and translation' *The Hindu* (India, 12 August 2024) https://www.thehindu.com/sci-tech/technology/supreme-court-confirms-use-of-ai-in-legal-research-and-translation/article68515713.ece#:~:text=Until%20August%205%2C%20the%20Supreme,using%20AI%2C%20the%20minister%20shared&text=Photo%20Credit:%20PTI-,The%20Supreme%20Court%20of%20India%20has%20confirmed%20that%20AI%20is,Court%20and%20High%20Court%20judgments. accessed on 05 January 2025

[13] Nupur Thapliyal, 'Supreme Court To Implement AI Tool To Generate Summary Of Pleadings: Delhi High Court ACJ Manmohan' (*Live Law,* 20 September 2024) https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-artificial-intelligence-in-law-pleadings-270115?fromIpLogin=88481.69819452817 accessed 03 January 2025

[14] ICMR, 'Ethical guidelines for application of Artificial Intelligence in Biomedical Research and Healthcare' (2023) https://www.icmr.gov.in/ethical-guidelines-for-application-of-artificial-intelligence-in-biomedical-research-and-healthcare accessed 04 January 2025

The emphasis on one such legislation must be pitched to help create a unified system of governance for data protection, risk mitigation, privacy concerns, protection tools associated with AI usage and address other social and ethical issues. One may point out that sector-specific laws will be much more proven optimising. However, the impact will be upon legal enforcement agencies to cope with the diverse rules and regulations issued by sectors in times of dispute and further rampage the burden of the judiciary.

III. BOON OR BANE?

AI uses algorithms from which it senses, learns, and reasons information. It uses a vast amount of information to provide the best experience online. It has been trained to utilise information, which also involves users' personal information, to generate outputs. Data collection is one of the avowal strategies used to create targeted advertising, make recommendations online, make decisions, etc. The issue is that there is no sight to know how and what kind of data has been put to use. Thinking about how one's personal information spirals around cyberspace without any definite restrictive patterns may also be too transnational for no one to be called upon accountability. Such causation is sufficient to raise concerns surrounding data privacy vis-à-vis the right to privacy. While hearing a PIL matter on unregulated AI and deepfakes, the Delhi High Court reflected a lack of legislation monitoring the complexities of these technologies. The court also pertained to the demand for legislation with extensive deliberation.[15]

This led to one of the significant concerns when technology is devised into reality, which is surrounding privacy. However, the correlation between privacy and technology has never been amiable and is not a new concern. Long identified by Warren and Brandeis in "The Right to Privacy" in the 1890s, when the telegraph was a well-known and widely used technology.[16] In the Indian perspective, the landmark judgment of 9 judges bench unanimously preached about privacy as a right and facet of Article 21 of the constitution.[17]

Aarogya Setu, India's COVID-19 contact-tracing app, used AI and location tracking to identify and inform users about potential exposure to the virus. The app collected sensitive data,

[15] Nupur Thapliya, 'Delhi High Court Seeks Centre's Stand On PIL Against Non-Regulation Of Artificial Intelligence And Deepfake Technologies' (*Live Law*, 04 December 2023) https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-pil-non-regulation-artificial-intelligence-deepfake-technologies-243638 accessed 02 January 2025

[16] Samuel D. Warren, and Louis D. Brandeis, 'The Right to Privacy.' (1890) 4(5) Harvard Law Review https://www.jstor.org/stable/1321160 accessed 02 January 2025

[17] *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1

including health status, GPS location, and Bluetooth interactions. Concerns arose over how this data was stored, processed, and shared, as well as the lack of transparency and privacy safeguards.

Another significant issue is the lack of vigilance of authorities in implementing laws for data protection threatened by AI-like technologies. The Digital Privacy Data Protection Act, 2023 (DPDP Act) has been in a long gestation period. Whereas the digital village is proactively demanding a continuance spectrum of data protection tools against posed threats, many countries have already started to precept legislation[18]. Law-field netizens are concerned that such delay will create a terminal loss in the information society. Apart from the delay in the implementation, questions like whether the law is adequate or not have been raised, directing problems with the legislation, such as a lack of stringent time-bounds on data fiduciaries to entertain queries of data principals, overwhelming reliance on other legislations for referencing, deep interventions of the central government over the appointment of the Data Protection Board, irregularities in the appointment of Data Protection Officer by data fiduciaries, etc.[19] Such shortcomings may result in hampered governance and the failure to relive justice against AI properly.

SEBI declared to take full responsibility for any AI-generated faulty output.[20] This lingers the trust away from the institution if they start to take the liability for a computing program, which can easily make mistakes based on errors in processing, software glitches, or bias in response. Asia Securities Industry & Financial Markets Association issued a response, pleading that faults of AI will put hurdling liabilities upon the institution.[21] Unnecessarily, institutions like SEBI are ready to accept faults of technology that seek extensive engagement to cope with increasing tasks to ensure efficiency.

[18] White & Case LLP, 'AI Watch: Global regulatory tracker' (2024) https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker#introduction accessed 03 January 2025
[19] John Brittas and Aneesh Babu, 'What Lies Beneath the PR Blitz on the New Data Protection Act?' **(***The Wire*, 27 August 2023**)** https://thewire.in/government/what-lies-beneath-the-pr-blitz-on-the-new-data-protection-act#:~:text=Exemption%20for%20processing%20children's%20data,or%20consent%20of%20their%20parents. Accessed 03 January 2025
[20] Lindecrantz, Pian Gi, and Zerbi (n 8)
[21] Asifma, 'ASIFMA Response to "Proposed amendments with respect to assigning responsibility for the use of artificial intelligence tools by Market Infrastructure Institutions, Registered Intermediaries and other persons regulated by SEBI".' (November 2024) https://www.asifma.org/wp-content/uploads/2024/11/2024-11-28-asifma-response-to-sebi-consult-on-responsibility-for-use-of-ai-final.pdf accessed 02 January 2025

A vast area of Intellectual Property Rights (IPR) is threatened, not only in India but across the globe, due to AI. It has been feared amongst IPR enthusiasts that the relevancy of inventiveness- innovation and novelty- in the world will be lost. A hardened layer of opaqueness in the data output is causing the insignificance of AI-based innovations related to IP, as idea sharing is a chief service to the world. Without a substantive sharing of information, how AI could come up with an invention is a predominant argument against AI. Statutory support is required to recognise AI as a holder of IP truly. A vital question needs to be addressed before navigating AI as a holder of IP: who has the authority to enjoy the benefits of rights due to the exquisite invention by an AI?

Concerns have been raised surrounding the constant threats posed by AI in the cohesive digital world. High-risk AI is a matter of concern, and to establish why India requires stringent laws to regulate AI, it is essential to identify concerns posed by AI. Each sector can lay down a list of issues. Such output can help authorities to formulate laws. A panel discussing issues can give direction to reproduce a law. A straight path can emerge from analysing various threats. It must also focus on fundamental rights, social and ethical issues, and economic costs to restore the previously mentioned compromised concerns.

IV. SKEPTICISM AND DEBATES

There are many reasons why India does not have any legislation managing AI. The list of reasons and steps taken in the exercise of germinating seeds for AI in the future of India is laid out.

1. AI is not mentioned in the technology-related legislations in the country. Information Technology Act of 2000 (IT Act) and subsequent rules do not discuss technologies like AI, ML, or LLM. Therefore, it is hard to incorporate these technologies into the existing legal framework as it will require a considerable chuck of addition. Instead, a separate law will be sufficient to bridge the lacuna. However, the Ministry of Electronics and Information Technology (MeitY) introduced the 'Proposed Digital India Act, 2023', which entails 'hi-risk' AI.[22] The honorary mention can influence the making of regulations to manage the risk that culminates from AI in the future.

[22] Ministry of Electronics and Information Technology (MeitY), 'Proposed Digital India Act' (2023) page 19 https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf accessed 02 January 2025

2. II. Since India does not have any formally established body exclusive to look over AI, there are other authorities and organisations like the NITI Aayog[23] and the MeitY[24] that have been handed over the task of looking after the AI management. These bodies have been taking care of AI in their way and creating rules occasionally to protect end users. For example, MeitY released 'advisories' in 2024,[25] which created tension among intermediaries. The said advisories were an issue, but the foremost pinpointing was whether MeitY could make guidelines for AI, which incidentally does not find scope under the IT Act. While the ministry is allowed to make guidelines for publishers in media, not for intermediaries, thus making such actions more tenuous.[26]

3. III. The government is not considering a separate AI regulatory body but may create an AI safety institute (AISI) to help set standards, frameworks and guidelines for AI development.[27] However, appointing a proper authority or officer(s) to look over AI in the country would be encouraged. AISI will not be a statutory body, and its delivered tasks could be amended with the vision of stakeholders in power. Manifesting control to anybody to regulate the affairs in whatever ways they may, exhilarate potentials. Such gesticulation is encouraged only if any permanent authority, to be established explicitly, is underway to take over the task on a primary basis. Encouraging the establishment of a body or a committee, perhaps under the leadership of an individual or group(s) of individuals knowledgeable enough to deal with AI regulation and deployment in the country.

4. Over-hauled guidelines and directories have been issued by the authorities to delineate the management of AI in India.[28][29] Despite constant efforts to make AI accustomed to India, it has been feared that the country may not be planning to introduce a law on AI-specific

[23] NITI Ayog, 'National Strategy for Artificial Intelligence' (2017) https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf accessed 02 January 2025
[24] MeitY, 'Due diligence by Intermediaries/Platforms under the Information Technology Act 2000 and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021' (15 March 2024) https://www.meity.gov.in/writereaddata/files/Advisory%2015March%202024.pdf accessed 02 January 2025
[25] Ibid.
[26] Information Technology 2000 s 13.
[27] Aditi Agrawal, 'Govt mulls setting up Artificial Intelligence Safety Institute' *Hindustan Times* (India, 13 October 2024) https://www.hindustantimes.com/india-news/govt-mulls-setting-up-artificial-intelligence-safety-institute-101728833433153.html#:~:text=The%20Indian%20government%20is%20considering,told%20stakeholders%20in%20a%20consultation accessed 02 January 2025
[28] NITI Ayog (n 23)
[29] MeitY (n 24)

regulation.[30] Instead, the government intends to stick to the approaches undertaken in the form of 'advisories' and guidelines. It is an imperative argument. The advisories and guidelines vehicled by the MeitY and NITI Ayog at the central level were "just" rules and regulations to provide a future framework for managing complex technologies like AI. "By not giving legislative backing to this advisory as yet, we have adopted a soft touch approach, which I think is required in the Indian context given the manifold use cases for India's unique problems and aspirations as a global leader on the adoption of public digital infrastructure to drive its economic growth," noted by a former MP Dr. Amar Patnaik.[31]

5. The technology is moving fast, but the laws are moving at a slow pace. This is not the first instance of derelictions of unbothered attitude.[32] Had India planned to formulate a regulation, it would have done it a brief time ago. India is examining the readiness of the people of the country to adapt to AI and its implications. The unsolicited delays have caused under-guided deployment of technology. India is ranked 10th in 'readiness' to adopt AI, keeping in account of economic acceptance in the society, infrastructure and future regulations.[33]

6. Many institutions are making autonomous efforts to regulate AI, indicating the country's vision to welcome AI and tackle associated challenges. This gives the lawmakers a breeding ground for a draft. Despite a righteous approach, the country is looking for a broader time on clock-watch. It is well known that India's lawmakers, including the judiciary, faced turmoil and backlash occasionally due to inefficient dedication to speedy work.[34] Such an approach dishonours people's trust and, at the outset of all, economic and technological lags and delays the appreciable justice to the needy ones. Despite the

[30] Shaoshan Liu, 'India's AI Regulation Dilemma' *The Diplomat* (South Asia, 27 October 2023) https://thediplomat.com/2023/10/indias-ai-regulation-dilemma/ accessed 03 January 2025

[31] Soibam Rocky Singh, 'Stringent regulations could hinder growth of AI in India: experts' *The Hindu* (New Delhi, 23 June 2024) https://www.thehindu.com/sci-tech/technology/overly-strict-regulations-could-hinder-ai-growth-in-india-caution-experts/article68320814.ece accessed 02 January 2025

[32] Krishnadas Rajgopal, 'Supreme Court flags 'serious lapses' in implementation of Protection of Women from Sexual Harassment Act' *The Hindu* (New Delhi, 13 May 2023) https://www.thehindu.com/news/national/supreme-court-flags-serious-lapses-in-protection-of-women-from-sexual-harassment-act/article66844150.ece accessed 03 January 2025

[33] Generosity AI Working Group, '*A Deep Dive into responses from the AI Readiness Survey in India*' (Great Tuesday, 2024) https://ai.givingtuesday.org/ai-readiness-survey-report-2024-india/ accessed 04 January 2025

[34] Law Pedia, 'Judicial delay in India' *Times of India* (India, 20 February 2023) https://timesofindia.indiatimes.com/readersblog/lawpedia/judicial-delay-in-india-50731/ accessed 02 January 2025

shortcomings on the part of the lawmakers at the central level, bodies like SEBI, Nasscom, etc, are working to bring a better approach to deal with issues arising from the usage of AI.

7. The government may hold off on making any regulatory law specifically for AI as there are sufficient laws to manage AI under various aspects. Pronounced in the G20 Ministerial Declaration her intention, India is looking forward to unlocking the full potential of AI before grubbing legislation.[35] Therefore, India's government has held off on AI-specific regulation, saying that there are enough existing laws around the priority areas of personal data protection and fraud. Instead, the government is developing a voluntary code for training, deployment, commercial sale, and rectification of misuse of LLMs and AI platforms. The code will use an informal directive principles approach with a 'risk-based' focus on the "robustness" of AI systems.[36]

It would be false to claim that the union has put forth no effort to calculate the laws specifically for AI. The actions mentioned earlier put forth efforts and the central's inclination to develop a law for AI soon. India is experimenting with the response of its soft laws in industry, civil society and various other sectors to build an AI-specific regulation in the near future rampantly. Rapidly growing technologies constantly pose risks to users countrywide. Therefore, it would be in the best interest of the public to put the efforts into action much sooner.

V. CONCLUSION

India has leverage by way of administrative to establish autonomous and statutory bodies under the acts passed by legislation at the central and state levels. Many institutions like SEBI, NMC, IRCTC, etc., make their own rules and regulations from time to time to manage their affairs. These bodies and institutions are empowered to regulate and manage their tasks with the essence of autonomy directed by statutory protection. Therefore, these bodies are also capable of restoring breaches, in the absence of centralised law, caused by AI deployed by way of formal rules for ease of doing business. However, AI is a computer program built to cohabit

[35] Prime Minister's Office, 'Declaration on Digital Public Infrastructure, AI and Data for Governance - Joint Communiqué by the G20 Troika (India, Brazil and South Africa), endorsed by several G20 countries, guest countries and international organizations' (December 2024) https://pib.gov.in/PressReleasePage.aspx?PRID=2074832 accessed 03 January 2025

[36] S Ronendra Singh, 'Government unlikely to regulate AI, instead working on a voluntary compliance code' *The Hindu Business Line* (New Delhi, 24 November 2024) https://www.thehindubusinessline.com/news/government-unlikely-to-regulate-ai-instead-working-on-a-voluntary-compliance-code/article68905275.ece accessed 05 January 2025

with the fast progress of tasks. It has been serving society, both in personal and professional lives. Private entities using AI from stakeholders and intermediaries are poised by the burden of violation of rights due to the lack of stringent laws in the country.

Despite its contribution, AI has been one of the reasons for the obliteration of the technology age. It is not yet too late to argue that machines like AI outweigh the benefits derived, but it is also not too late to say for the demand for AI-based regulations. Many countries across the globe have scored to bring up specific rules dealing with risks posed by AI, focusing on better usage and advancement of technologies like AI. Not only management but accuracy, innovation, and governance are some of the critical features incorporated by laws of foreign.

Now that laws across the globe have started to emerge, India can use those as model laws to build laws for the country, incorporating infrastructural differences, needs, demands, and challenges. Nonetheless, making existing foreign companies sponsored AIs in the country more responsible and developing futuristic plough in the country to flourish the technological advancement. Recently, MeitY released a report[37] to align AI Governance along the lines of human rights, fairness, transparency, accountability, safety against bias and discrimination, and privacy compliance. It targets stakeholders from government, industry, academia and researchers, and civil society to adhere to the usage of AI based on the lines of the report. This AI governance report is critical to fostering trust and sustainability in AI adoption. While significant progress has been made, continuous collaboration and adaptation are essential to address emerging challenges and ensure AI systems serve humanity effectively and equitably.

[37] MeitY, 'Report on AI governance guidelines development' (January 2025) https://indiaai.s3.ap-south-1.amazonaws.com/docs/subcommittee-report-dec26.pdf accessed 08 January 2025

DIGITAL REPLICAS OF DECEASED INDIVIDUALS AND THE DPDP ACT: ADDRESSING INDIA'S LEGAL GAPS THROUGH INTERNATIONAL COMPARISONS

— Akash Kumar Sahu and Arhant[*]

ABSTRACT

AI technology has made it possible to create digital copies of people who have passed away. These digital replicas, made from photos, videos, and personal data, can help families keep memories alive and even interact with virtual versions of their loved ones. But this technology also brings serious problems, like using someone's likeness without permission or exploiting it for profit. This article examines the effectiveness of India's Digital Personal Data Protection (DPDP) Act in safeguarding these digital identities or digital data posthumously. Although the DPDP Act emphasizes data privacy and consent, it lacks specific provisions addressing the rights and protections of digital replicas after death. By contrast, California civil code section 3344.1 provides a more robust framework, with defined rules for inheriting and controlling digital likenesses. Through the case studies and practical scenarios, the paper shows the practical challenges of managing digital legacies in this interconnected world. Recommendations include amending the DPDP Act to incorporate explicit provisions for posthumous data rights, adopting best practices from California's legislation, and fostering cross-border collaboration to address the concern.

This paper also proposes several key changes, including recognizing digital assets as inheritable, establishing mechanisms for digital legacy management, and introducing guidelines to prevent misuse. These additions would help ensure that digital identities are treated with

[*] The authors are students at National Law Institute University, Bhopal (NLIU).

respect, along with honouring individuals' wishes and protecting their legacy in a digital era.

Keywords: Digital Data, Deceased individuals, Digital Personal Data Protection Act (DPDP Act), California AB 1836, Posthumous digital persona, Ethical concerns Consent and privacy, Commercial exploitation, Inheritance of digital data, Digital legacy management, AI and deepfake technology, Emotional manipulation.

INTRODUCTION

"*Privacy is not an option, and it shouldn't be the price we accept for just getting on the internet.''* – Gary Kovacs, Former CEO of AVG Technologies[1].

In recent years, artificial intelligence (AI) has made it possible to create something that once seemed like science fiction: digital replicas of people who have passed away. These lifelike avatars, built from personal data like photos, videos, and voice recordings, can mimic the appearance and behaviour of deceased individuals. For many, this technology offers a way to preserve memories and feel connected to loved ones who are no longer with us. But it also raises serious questions about privacy, consent, and ethics.

Think a world where a company uses a digital version of a deceased celebrity to sell products, or a grieving family discovers that their loved one's likeness has been turned into a virtual avatar without their permission. These scenarios are no longer hypothetical, they are happening today. A 2019 survey by the Pew Research Centre found that 79% of Americans are worried about how companies use their personal data, with 36% saying they are "very concerned."[2]

These concerns become even more complicated when dealing with digital replicas after death. India's *Digital Personal Data Protection Act (DPDP Act)*[3] was created to protect personal data in the digital age. But does it go far enough to address the challenges posed by digital replicas

[1] US Ignite, *US Ignite Civic Trust Guide: Privacy in Civic Tech* (2021) https://www.us-ignite.org/wp-content/uploads/2021/06/USIgnite-Civic-Trust-Guide_Sec3_Privacy.pdf accessed 9 December 2024
[2] Brooke Auxier and others, 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' (Pew Research Center, 15 November 2019) https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/ accessed 14 March 2025.
[3] Digital Personal Data Protection Act 2023 (India).

of deceased individuals? While the DPDP Act [4]focuses on privacy and consent during a person's lifetime, it doesn't clearly address what happens to digital identities after death. This leaves a gap that could allow misuse, such as unauthorized commercial use or emotional manipulation.

This paper explores how well the DPDP Act[5] handles these issues and compares it to laws like *California civil code section 3344.1*[6] (California's *AB 1836),*[7] which provides stronger protections for digital replicas after death. By looking at real examples and practical challenges, we aim to highlight the need for better legal frameworks in India. We also propose changes, such as updating the DPDP Act to include posthumous data rights and creating systems for managing digital legacies. After all, in a world where our digital footprints outlive us, it's essential to ensure that these footprints are treated with the same care and respect as our physical legacies.

DEFINING DIGITAL REPLICAS OF DECEASED INDIVIDUALS

Digital replicas are lifelike simulations of a person's voice, appearance, or behaviour, created using advanced digital technology.[8] Think of them as virtual copies of real people, so accurate that they're easily recognizable as the individual they're based on. These replicas are built using personal data like photos, voice recordings, signatures, or even mannerisms, pieced together to recreate a person's identity in the digital world.

The term "posthumous digital persona" is often used to describe digital replicas of deceased individuals. As defined in California's *Civil Code Section 3344.1 (2)(b)*,[9] a posthumous digital persona is a lifelike digital representation of someone who has passed away. Similarly, the *International Association of Privacy Professionals (IAPP)* describes it as a "digitally reconstructed likeness of a deceased person, used in digital media, marketing, entertainment, or social interactions."[10]

[4] ibid.
[5] ibid.
[6] California Civil Code s 3344.1.
[7] California Assembly Bill 1836 (2023) https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1836 accessed 14 March 2025.
[8] New York Senate Bill S7676B (2023) https://www.nysenate.gov/legislation/bills/2023/S7676/amendment/B accessed 14 March 2025.
[9] California Civil Code s 3344.1(2)(b).
[10] Lee Poskanzer, Sharon Hartung, and Jennifer Zegel, 'The Birth of Postmortem Privacy' (IAPP, 22 June 2021) https://iapp.org/news/a/the-birth-of-postmortem-privacy accessed 21 October 2024.

New York has also taken steps to regulate this emerging technology. The *New York Senate Bill 7676B*, which took effect on January 1, 2025, defines a "digital replica" as "a digital simulation of the voice or likeness of an individual" that, to an average person, "so closely resembles" the individual that it's virtually indistinguishable from the real thing.[11] This law regulates contracts for creating and using digital replicas, ensuring that individuals have control over how their likeness is used, even after death.

In simpler terms, a digital replica is like a virtual "ghost" of a person, a version of them that can exist online, in movies, or even as an AI chatbot.[12] For example, companies like *Replika* and *Eternalize* use AI to create avatars that mimic the personality, voice, and appearance of deceased individuals, allowing families to "interact" with their loved ones long after they're gone.[13]

But while this technology offers incredible possibilities, it also raises serious questions. Who gets to decide how a digital replica is used? What happens if it's created or used without permission? And how do we ensure that these digital versions respect the dignity and wishes of the person they represent?

As technology continues to advance, these questions become even more urgent. Digital replicas are no longer just a futuristic idea, they're here, and they're forcing us to rethink how we define identity, privacy, and legacy in the digital age.

DATA ANALYSIS, STATISTICS AND REAL CASES: THE USE AND MISUSE OF DIGITAL REPLICAS

As AI technology continues to evolve, the creation of digital replicas of deceased individuals has become more accessible and widespread. While this innovation offers meaningful ways to preserve memories, it also opens the door to ethical, privacy, and security concerns. Let's

[11] New York Senate Bill S7676B (2023) https://www.nysenate.gov/legislation/bills/2023/S7676/amendment/B accessed 14 March 2025.
[12] Will Douglas Heaven, 'Seeing Double: AI Births Digital Humans' (MIT Technology Review, 29 September 2022) https://www.technologyreview.com/2022/09/29/1060425/seeing-double-ai-births-digital-humans/ accessed 14 March 2025.
[13] Alexander Gerner, 'AI Heritage Avatars' (ResearchGate, 29 November 2024) https://www.researchgate.net/publication/386273899_AI_Heritage_Avatars accessed 14 March 2025.

explore the growing popularity of digital replicas, the risks of misuse, and real-world cases that highlight the challenges of this technology.

A. Growing Popularity of Digital Replicas

The demand for digital replicas is on the rise, driven by a mix of emotional needs and technological advancements. According to a *Pew Research Center* study, 53% of U.S. adults have reported some form of interaction with deceased family members, whether through dreams, memories, or even digital means. About 34% of Americans say they've felt the presence of a deceased relative in the past year, and 28% have shared personal life events with them.[14]

The table below shows the findings from a Pew Research Center survey on Americans' interactions with deceased relatives. [15]

Survey Findings on Interactions with Deceased Relatives	***Percentage of Respondents***
Experienced at least one interaction with a deceased relative in the past year	44%
Felt the presence of a dead family member in the past 12 months	34%
Told a dead relative about their life in the past 12 months	28%
Had a deceased family member communicated with them in the past 12 months	15%

Demographic Breakdown	***Percentage***
Women who reported at least one of the above experiences in the past 12 months	53%

[14] Pew Research Center, 'Many Americans Report Interacting With Dead Relatives in Dreams or Other Ways' (Pew Research Center, 23 August 2023) https://www.pewresearch.org/short-reads/2023/08/23/many-americans-report-interacting-with-dead-relatives-in-dreams-or-other-ways/ accessed 21 October 2024.

[15] Pew Research Center, *Views on the Afterlife* (23 November 2021) https://www.pewresearch.org/religion/2021/11/23/views-on-the-afterlife/ accessed 27 October 2024.

Men who reported at least one of the above experiences in the past 12 months	35%

These numbers show a deep human desire to stay connected to those we've lost. Digital replicas tap into this desire by offering a way to "interact" with loved ones through lifelike avatars. But as this technology grows, so do the risks of misuse.

B. Market Expansion and Ethical Challenges in the Asia Pacific

The Asia Pacific region is leading the charge in adopting digital avatar technology. With a projected *Compound Annual Growth Rate (CAGR) of 54.2%* from 2024 to 2030, the region is seeing rapid advancements in AI, augmented reality (AR), and facial recognition. Countries like China, Japan, and India are at the forefront, driven by rising internet access, smartphone usage, and a cultural openness to virtual experiences.[16]

The table below provides an overview of key trends in the Asia Pacific Digital Avatar Market from 2024 to 2030.

Country/Region	**CAGR (2024-2030)**	**Key Factors Driving Growth**	**Additional Information**
Asia Pacific (Overall)	54.2%	- Increasing internet penetration - Rising smartphone usage - Growth in the e-commerce activities - Focus on technology and innovation in she tart-up ecosystem	- Region includes technologically advanced countries like Japan, South Korea, China, and Singapore. - Digital avatars adopted in marketing, customer interactions, and virtual experiences.
China	53%	- Growth of AI-generated digital avatars	- Country leveraging AI for digital avatar creation.

[16] Grand View Research, *Asia Pacific Digital Health Market Report* (2021) https://www.grandviewresearch.com/industry-analysis/asia-pacific-digital-health-market-report accessed 27 October 2024.

		- Focus on artificial intelligence for creating realistic, interactive digital human representations	
India	56.4%	- Investment in the advanced technologies like AI, AR, VR, facial recognition, and motion tracking - Focus on enhancing user experiences	- Companies are driving innovation and user engagement with cutting-edge digital avatar technologies.

The Asia Pacific region is quickly becoming a global leader in digital avatar technology. From 2024 to 2030, the market is expected to grow at an impressive rate of 54.2% per year.[17] This growth is driven by advancements in artificial intelligence (AI), augmented reality (AR), and facial recognition technologies. Countries like China, Japan, and India are leading the way, thanks to increasing internet access, widespread smartphone use, and a cultural openness to virtual experiences.

C. Misuse of Digital Replicas

Digital replicas are like a double-edged sword. On one side, they offer comfort and connection. On the other, they can be misused in ways that hurt people, exploit memories, and even manipulate society. Without clear rules and regulations, this powerful technology can easily go wrong. Let us see real examples that shows how digital replicas can be misused and why we need to act now to prevent harm.

i. Commercial Exploitation and Lack of Consent: The Anthony Bourdain Case

Anthony Bourdain was a chef, storyteller, and a voice many loved. After his passing in 2018, his voice was brought back to life in the 2021 documentary *Roadrunner: A Film About Anthony Bourdain*. Using AI, filmmakers recreated Bourdain's voice to read words he had written but never recorded.[18] It sounds like a tribute, right?

[17] ibid.
[18] Helen C Boucher, *'The Ethics of Using A.I. to Recreate Anthony Bourdain's Voice'* (The New York Times, 16 July 2021) https://www.nytimes.com/2021/07/16/movies/anthony-bourdain-ai-voice.html accessed 27 October 2024.

But here's the problem: Bourdain's family wasn't asked for permission. His ex-wife, Ottavia Busia-Bourdain, said she was shocked and felt it was wrong. She believed Bourdain wouldn't have agreed to it. The filmmakers claimed they had permission from his literary agent, but that wasn't enough for his family.[19]

This case shows how digital replicas can cross ethical lines. Without clear consent, even well-meaning projects can hurt the people left behind. It also raises questions: Who gets to decide how a deceased person's voice or likeness is used? And how do we make sure their wishes are respected?

ii. Political Manipulation and Misinformation: The Case of Recreated Deepfakes in Election Campaigns

In 2020, during an election campaign in India, a deepfake video of politician Manoj Tiwari went viral. The video showed he was speaking in the Haryanvi dialect, a speech he never actually gave.[20] The AI-generated video was designed to connect with local voters and was shared widely on social media.

While he was alive and aware of the video, this case is a warning. Imagine if a deceased politician's digital replica was used to spread false messages or manipulate voters. The potential for misuse is huge, especially in politics where trust is everything. This isn't just about one election but it's about the future. Without rules and regulations, digital replicas could become tools for spreading lies and dividing people.

iii. Emotional Exploitation: The Rise of "Ghostbots" and the Case of Roman Mazurenko

The story of Roman Mazurenko, a Russian entrepreneur who died in 2015, shows how digital replicas can deeply affect grieving families. After his passing, Roman's friend Eugenia Kuyda, who co-founded the AI chatbot company Replika, used his old text messages to create a "ghostbot" a digital version of Roman that people could interact with. For some, this brought comfort, as it felt like a way to keep a part of him alive.[21] But for others, including his family,

[19] ibid.
[20] Will Knight, 'An Indian Politician Is Using Deepfakes to Try and Win Voters' (MIT Technology Review, 19 February 2020) https://www.technologyreview.com/2020/02/19/868173/an-indian-politician-is-using-deepfakes-to-try-and-win-voters/ accessed 28 October 2024.
[21] F Donoghue, 'Chatting with the Dead: How AI Chatbots Could Transform Grief and Memory' (*The MIT Press Reader*, 15 March 2023) https://thereader.mitpress.mit.edu/chatting-with-the-dead-chatbots/ accessed 11 March 2025.

it felt unsettling. They wondered if Roman would have agreed to this kind of digital re-creation in the first place.[22] This story shows how digital replicas can bring both comfort and challenges. On one hand, they can help people deal with loss and feel closer to loved ones who are no longer here. On the other hand, they can sometimes feel intrusive or disrespectful, especially if the person never agreed to being recreated digitally. It is a reminder that as technology grows, it should always respect a person's dignity, whether they're alive or have passed away. Balancing innovation with care and respect is essential to ensure these tools truly help people without crossing ethical lines.

iv. Intellectual Property Infringement: The Case of Audrey Hepburn in Advertisements

Audrey Hepburn, a famous actress, passed away in 1993. But in 2013, she "appeared" in a commercial for Galaxy chocolate. Using AI and CGI, filmmakers recreated her 1950s look, making her the face of the ad. While Hepburn's estate approved the project, it sparked a debate. Was this a beautiful tribute to her legacy or a way to use her image for profit? Critics argued that it reduced Hepburn to a marketing tool, while supporters saw it as a celebration of her elegance.[23] This case highlights the fine line between honouring someone's memory and exploiting it. It also raises questions about who controls a deceased person's image and for how long.

D. The Bigger Picture: Why We Need Rules

These stories show the dark side of digital replicas. From using someone's voice without permission to spreading fake messages or exploiting a celebrity's image, the risks are real. And the common thread in all these cases is consent. Who gets to decide how a digital replica is used? Is it the person before they passed away? Their family? Or companies looking to make money? Without clear laws, these questions remain unanswered. That's why we need laws and regulations that protect people's rights, respect their dignity, and prevent misuse.

[22] Call for Safeguards to Prevent Unwanted Hauntings by AI Chatbots of Dead Loved Ones' (University of Cambridge, 29 November 2023) https://www.cam.ac.uk/research/news/call-for-safeguards-to-prevent-unwanted-hauntings-by-ai-chatbots-of-dead-loved-ones accessed 14 March 2025.

[23] Olivia Bergin, *'How A CGI Audrey Hepburn Wound Up In A Chocolate Commercial'* (Refinery29, 11 February 2013) https://www.refinery29.com/en-us/2013/02/43712/audrey-hepburn-chocolate-commercial accessed 27 October 2024.

Digital replicas are here to stay. They can bring comfort, preserve memories, and even keep legacies alive. But they must be used responsibly. By learning from these real-life examples, we can create a future where technology honours people, not exploits them.

I. LEGISLATIVE PROTECTIONS FOR DIGITAL REPLICAS OF DECEASED INDIVIDUALS IN CALIFORNIA[24]

In California, the law that protects digital replicas of deceased people is mainly found in Section 3344.1 of the California Civil Code.[25] This law protects the rights of individuals by ensuring that their name, voice, signature, photograph, or likeness cannot be used for profit without permission after they die. If someone uses these elements without authorization for commercial purposes, they face serious legal consequences. The penalties include paying at least $750 or the actual damages caused, plus any profits made from the unauthorized use.[26]

California law clearly defines a "digital replica" as a copy of a deceased person's voice or likeness that people can easily recognize.[27] If someone produces or shares a digital replica related to the deceased person's past work, they face higher penalties of at least $10,000 or actual damages.[28] This part of the law shows California's dedication to protecting the reputation and likeness of individuals even after they pass away. It highlights the need for permission when using their intellectual property.

The law views these rights as property rights that can be transferred freely. When a person dies, their likeness rights go to specific people as stated in the law. The surviving spouse, children, or other relatives can use these rights, allowing them to profit from the deceased's likeness.

[24] California Assembly Bill 1836 (AB 1836) (2023).
[25] California Civil Code § 3344.1 (2023) https://casetext.com/statute/california-codes/california-civil-code/division-4-general-provisions/part-1-relief/title-2-compensatory-relief/chapter-2-measure-of-damages/article-3-penal-damages/section-33441-effective-until-112025-using-deceased-persons-name-voice-signature-photograph-or-likeness accessed 21 October 2024.
[26] California Civil Code § 3344.1 (2023) https://advance.lexis.com/open/document/openwebdocview/Cal-Civ-Code-3344-1/?pdmfid=1000522&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5J6R-DKP1-66B9-84VX-00000-00&pdcomponentid=4867 accessed 21 October 2024.
[27] California Civil Code § 3344.1 (2023) https://advance.lexis.com/open/document/openwebdocview/Cal-Civ-Code-3344-1/?pdmfid=1000522&pddocfullpath=%2Fshared%2Fdocument%2Fstatutes-legislation%2Furn%3AcontentItem%3A5J6R-DKP1-66B9-84VX-00000-00&pdcomponentid=4867 accessed 21 October 2024.
[28] California Assembly Bill 1836, 2023 https://legiscan.com/CA/text/AB1836/id/2984163 accessed 21 October 2024.

However, if there are no heirs or if the rights are not transferred through a contract or will, these rights will end.[29]

The law also states that using a deceased person's likeness for news, public affairs, or sports broadcasts does not need consent. This allows for free expression while still respecting the rights of the deceased. Furthermore, any claims about using a deceased person's likeness must be registered with the Secretary of State. This makes such claims public records to ensure transparency in using these rights.

Importantly, the law limits claim to those made within 70 years after a deceased person's death.[30] This balance protects the interests of living individuals while respecting the rights of those who have passed away. By creating clear rules for using digital replicas, California aims to maintain the dignity and legacy of deceased individuals while adapting to the challenges of intellectual property in the digital world.[31]

LEGAL GAPS IN DIGITAL REPLICA PROTECTIONS IN INDIA: EVALUATING THE DIGITAL PERSONAL DATA PROTECTION ACT

The Digital Personal Data Protection Act (DPDPA)[32] in India sets out as important legislation for protecting personal data, but when it comes to protecting digital replicas, the law has some major gaps.

Firstly, one of the strengths of the DPDPA[33] is its emphasis on consent for processing personal data, as outlined in Section 6,[34] which mandates that personal data should only be collected with the explicit consent of the data subject. This provision is essential because it ensures individuals have control over how their data is collected, used, and processed during their

[29] 'How to Transfer Property to Legal Heir After Owner's Death' (The Economic Times, 5 September 2023) https://economictimes.indiatimes.com/wealth/legal/will/how-to-transfer-property-to-legal-heir-after-owners-death/articleshow/103453738.cms?from=mdr accessed 14 March 2025.
[30] Digital Media Law Project, 'California Right of Publicity Law' (Digital Media Law Project, 2023) https://www.dmlp.org/legal-guide/california-right-publicity-law accessed 21 October 2024.
[31] ibid.
[32] Digital Personal Data Protection Act 2023 (India).
[33] ibid.
[34] Digital Personal Data Protection Act 2023 (India), s 6.

lifetime. [35]In the context of digital replicas, this requirement allows individuals to dictate whether their digital likeness can be created or used. However, Section 14(1)[36] also highlights that individuals have the right to nominate a person to manage their data after death. While this is a positive step, the DPDPA[37] remains silent about what happens if the individual fails to make such a nomination. As AI technology continues to evolve, the ability to create highly accurate digital replicas of deceased individuals grows, and without clear guidance, it is unclear how these replicas should be protected. In contrast, California's Civil Code Section 3344.1(d)[38] offers a model that addresses this issue. This law outlines a structured approach to managing the rights to a deceased person's name, voice, and likeness. It establishes a clear order of succession, starting with the surviving spouse, followed by children, and in some cases, grandchildren. If there is no surviving spouse, the rights go to the children or the children of any deceased children, and if no immediate family members are left, the rights go to the parents. This clear framework provides a legal mechanism for handling digital replicas after death by ensuring that the deceased person's likeness is managed by someone with legal authority. For example, when the rights to a deceased celebrity's digital likeness are handled according to a structured succession plan, the family members can manage or use it as they see fit.

Secondly, the DPDPA[39] enforces strict guidelines for data fiduciaries who are responsible for handling personal data as laid out in Section 8. [40]. It holds these companies accountable for ensuring transparency, security, and compliance with privacy standards as discussed in the case of *Karthick Theodore vs The Registrar General.*[41] This framework helps prevent the unauthorized creation or misuse of personal data, including data used to form digital replicas. However, the Act does not directly regulate the creation or management of digital replicas. Without a specific framework governing digital replicas, data fiduciaries could potentially create or use virtual identities based on personal data for purposes not fully understood by the

[35] Latham & Watkins LLP, 'India's Digital Personal Data Protection Act 2023 vs the GDPR: A Comparison' (2023) https://www.lw.com/admin/upload/SiteAttachments/Indias-Digital-Personal-Data-Protection-Act-2023-vs-the-GDPR-A-Comparison.pdf accessed 14 March 2025.
[36] Digital Personal Data Protection Act 2023 (India), s 14(1).
[37] Digital Personal Data Protection Act 2023 (India).
[38] California Civil Code § 3344.1(d).
[39] Digital Personal Data Protection Act 2023 (India).
[40] Ministry of Electronics and Information Technology, *Digital Personal Data Protection Act 2023* (India) https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf accessed 27 October 2024.
[41] *Karthick Theodore v The Registrar General* WP(MD) No. 18884 of 2023 (Madras HC, 28 September 2023) https://www.livelaw.in/pdf_upload/karthick-v-registrar-general-525727.pdf accessed 27 October 2024.

data subject. This gap in the DPDPA[42] makes it difficult to ensure that digital replicas are created and used in ethical and transparent ways.

Thirdly, a significant strength of the DPDPA[43] is the empowerment it provides individuals by giving data subjects, the right to correct or delete their personal data, as outlined in Section 12[44]. This gives individuals control over their digital identities, ensuring that their personal data or digital replicas can be modified or erased to avoid misrepresentation or harm. However, this right ceases upon the individual's death if they have not nominated a representative under Section 14(1) of the Act,[45] as the DPDPA[46] does not provide any provisions for managing the personal data of deceased persons in such cases. This oversight leaves digital replicas of the deceased vulnerable to exploitation. For example, after a person passes away, their digital replica could be used for identity theft, unauthorized commercial purposes, or even to alter their digital legacy without their consent. The lack of posthumous control over data and digital replicas creates significant ethical concerns. Without provisions for digital succession or inheritance just like intestate succession under Hindu Succession Act, 1956,[47] the DPDPA [48]leaves digital identities in a legal limbo, risking misuse or harm to the deceased's legacy and the emotional well-being of their family members.

Fourthly, while the DPDPA[49] holds data fiduciaries accountable for their actions and encourages responsible behaviour as per section 8 of the act,[50] it does not provide adequate guidance on the management of digital replicas of deceased individuals. The lack of clear legal or ethical guidelines in the DPDPA[51] makes it unclear how companies should handle such sensitive matters, potentially leading to exploitation or emotional harm to the deceased's family.

[42] Digital Personal Data Protection Act 2023, Act No. 22 of 2023 (India).
[43] ibid.
[44] Digital Personal Data Protection Act 2023 (India), s 12.
[45] Digital Personal Data Protection Act 2023 (India), s 14(1).
[46] Digital Personal Data Protection Act 2023 (India).
[47] Hindu Succession Act 1956 (India).
[48] Digital Personal Data Protection Act 2023 (India).
[49] ibid.
[50] Digital Personal Data Protection Act 2023 (India), s 8.
[51] Digital Personal Data Protection Act 2023 (India).

Fifthly, the DPDPA[52] includes provisions for cross-border data transfers under Section 16,[53] allowing the sharing of personal data with other countries under specific conditions. However, it does not specify how digital replicas created using such data should be regulated when shared internationally. As digital replicas and AI-generated likenesses become more common, the international nature of digital data poses a significant challenge for data protection. If personal data used to create digital replicas is transferred to countries with weaker data protection laws, enforcing Indian data protection standards becomes difficult. This could lead to the exploitation of digital replicas in jurisdictions where privacy laws are less stringent. The Cambridge Analytica Scandal is a prime example of how cross-border data transfers can lead to the misuse of personal data.[54] Without proper legal structures to regulate the use of digital replicas across borders, the DPDPA[55] risks leaving individuals' digital identities vulnerable to exploitation on a global scale.

Lastly, while the DPDPA[56] positions itself as a forward-thinking Act that seeks to address India's data challenges, it remains ill-equipped to handle emerging technologies like AI, machine learning, and deepfakes. As digital replicas become more lifelike and widespread, the DPDPA[57] must evolve to account for issues such as ownership, inheritance, and ethical considerations related to posthumous digital identities. Without clearer provisions that address these issues, the DPDPA[58] may struggle to keep pace with technological advancements that involve the creation and use of digital replicas. The Act[59] needs to be updated to include specific guidelines that not only regulate the creation and use of digital replicas but also ensure that individuals have control over their digital likenesses, even after death.

[52] Digital Personal Data Protection Act 2023 (India).
[53] Digital Personal Data Protection Act 2023 (India), s 16.
[54] Ioana Loredana Tanase, *Cambridge Analytica in the Era of Surveillance Capitalism: The Impact on Democratic Structures - Digital Surveillance and the Private Sector* (Leiden University 2019) https://studenttheses.universiteitleiden.nl/access/item%3A3191049/view accessed 14 March 2025.
[55] Digital Personal Data Protection Act 2023 (India).
[56] ibid.
[57] ibid.
[58] ibid.
[59] ibid.

COMPARATIVE ANALYSIS OF POSTHUMOUS DIGITAL DATA LAWS ACROSS VARIOUS COUNTRIES

Country	**Relevant Law/Act**	**Posthumous Data Rights**	**Consent for Digital Replica**	**Inheritance of Digital Data**
United States (California)	California Civil Code §3344.1 (AB 1836)[60]	Protects the deceased's likeness, requiring estate consent for commercial use, with fines for violations.	Requires explicit consent from the estate for commercial use of digital replicas.	Estate inherits rights to control likeness up to 70 years posthumously.[61]
European Union	General Data Protection Regulation (GDPR)[62]	GDPR applies only to living individuals, as stated in Recital 27 and Article 4(1)- there is no statutory provision for posthumous data rights at the EU level.[63]	Consent for data processing is required only during an individual's lifetime. Since Recital 27[64] and Article 4(1)[65] define personal data as relating to living	There is no unified EU provision for digital inheritance. Inheritance issues are left to each Member State's national law since the GDPR does not address the transfer of digital assets after death (no specific article in the GDPR covers this).

[60] California Civil Code §3344.1 (2023) (AB 1836).
[61] ibid.
[62] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR) [2016] OJ L119/1.
[63] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, recital 27 and art 4(1).
[64] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, recital 27.
[65] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 4(1).

			individuals, there is no legal basis for posthumous consent regarding digital replicas.	
South Korea	Personal Information Protection Act (PIPA) 2011[66]	PIPA defines "personal information" as data relating to living individuals only (see Article 2(1) of PIPA).[67]Consequently, no legal provision exists within PIPA for the protection of personal data after death.	Although PIPA[68] mandates explicit, informed consent for data processing during life (e.g., Article 15[69]), it does not include any mechanism for obtaining or managing consent for digital replicas after death.	PIPA[70] does not contain any dedicated section addressing digital inheritance. Digital assets are not specifically treated in PIPA[71], so their transfer upon death is managed under general inheritance laws (PIPA does not address this modern digital issue).

[66] Personal Information Protection Act 2011 (South Korea), Act No. 10465.
[67] Personal Information Protection Act 2011 (South Korea), art 2(1).
[68] Personal Information Protection Act 2011 (South Korea).
[69] Personal Information Protection Act 2011 (South Korea), art 15.
[70] Personal Information Protection Act 2011 (South Korea).
[71] Personal Information Protection Act 2011 (South Korea).

United Kingdom	Data Protection Act 2018 (DPA)[72]	Applies during an individual's life only.	Requires consent but is unclear for posthumous use.	Generally left to service provider policies and private arrangements.
India	Digital Personal Data Protection Act (DPDPA) (2023)[73]	No explicit automatic posthumous data rights. However, under Section 14(1)[74], an individual may nominate another person to exercise their data rights after death.	Requires explicit consent for data processing under Section 6 [75]during life. The DPDPA is silent on the creation or use of digital replicas posthumously.	Section 14(1) [76]permits digital inheritance through nomination. If no nomination, there is no legal provision to govern posthumous data control.
France	Digital Republic Act[77] & GDPR[78]	Based on GDPR (Recital 27 [79]and Article 4(1)), [80]French law applies data protection both	Consent is explicitly required during life per the GDPR[81]. However, the	Based on GDPR (Recital 27 and Article 4(1)),[84] data protection applies only to living individuals; however, French law, through the Digital

[72] Data Protection Act 2018, c 12.
[73] Digital Personal Data Protection Act 2023, Act No. 22 of 2023 (India).
[74] Digital Personal Data Protection Act 2023 (India), s 14(1).
[75] Digital Personal Data Protection Act 2023 (India), s 6.
[76] Digital Personal Data Protection Act 2023 (India), s 14(1).
[77] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique* (Digital Republic Act) (France).
[78] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR) [2016] OJ L119/1.
[79] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, recital 27 and art 4(1).
[80] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, art 4(1).
[81] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
[84] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, recital 27 and art 4(1).

		to living and posthumous individuals.	GDPR[82] does not provide but the Digital Republic Act provides guidance for managing digital replicas after death (see Article 40-1[83]),	Republic Act (specifically, Article 40-1[85] of the amended French Data Protection Act), provides a mechanism for individuals to set posthumous directives for managing their personal data. In the absence of such directives, families may request the deletion of a deceased person's account.
Japan	Act on Protection of Personal Information (APPI)[86]	APPI defines personal information as data relating to a living individual (Article 2(1) of APPI[87]). Protection ends at death, so there is no legal provision for posthumous data rights.	Consent is required during life under APPI; however, the Act does not extend any rules for handling consent for digital replicas once the individual dies (APPI Article 15[88] and related	APPI does not include any specific legal framework for digital inheritance. Digital assets are managed on a case-by-case basis or via private agreements, as there is no statutory section addressing this issue.

[82] ibid.
[83] French Digital Republic Act 2016, art 40-1.
[85] French Digital Republic Act 2016, art 40-1.
[86] Act on the Protection of Personal Information 2003 (Japan), Act No. 57 of 2003.
[87] Act on the Protection of Personal Information 2003 (Japan), art 2(1).
[88] Act on the Protection of Personal Information 2003 (Japan), art 15.

			provisions do not cover the posthumous context).	

INDIAN JUDICIAL PRECEDENTS ON POSTHUMOUS DIGITAL IDENTITY AND DATA RIGHTS

In India, the law is still figuring out how to deal with what happens to your digital identity and personal data after you die. Right now, courts have made it clear that the right to privacy ends with a person's life.

Firstly, in the case of *Deepa Jayakumar v. A. L. Vijay & Others*,[89] the Madras High Court dealt with the issue directly. The case involved a movie titled "Thalaivi," based on the life of the late Chief Minister J. Jayalalithaa. Deepa Jayakumar, her niece, tried to stop the release of the movie, claiming it violated her aunt's privacy and posthumous rights. However, the court clearly stated that privacy or reputation earned by a person during their lifetime ends with their death. The court went on to observe:

"Para 37: A privacy or reputation earned by a person during his or her lifetime, extinguishes with his or her death. After the death of a person, the reputation earned cannot be inherited like a movable or immovable property by his or her legal heirs. Such personality right, reputation or privacy enjoyed by a person during his lifetime comes to an end after his or her lifetime. Therefore, we are of the opinion that 'posthumous right' is not an alienable right and the appellant/plaintiff is not entitled for an injunction on the ground that the 'posthumous right' of her aunt is sought to be sullied by the respondents/defendants by reason of the release of the film titled as 'Thalaivi.'"[90]

[89] Deepa Jayakumar v A L Vijay & Others [2020] 1 CTC 670 (Madras HC)
[90] Deepa Jayakumar v A L Vijay [2020] 1 CTC 670 (Madras HC) https://indiankanoon.org/doc/9075307/ accessed 14 March 2025.

This judgment made it clear that posthumous rights are not inheritable or transferrable, unlike physical property.

Secondly, the Delhi High Court, in the case of *Krishna Kishore Singh v. Sarla A. Saraogi & Others (2021)*,[91] came to the same conclusion. This case involved Sushant Singh Rajput's father, who was upset about movies and shows being made about his late son without the family's permission. The court ruled that after someone dies, their personality rights (such as control over their name, image, and story) do not continue unless there is a specific law to protect them. The court did say that if something defamatory or harmful was done, action could still be taken, but normal personality rights do not survive death.

These cases show a clear problem. While living people in India have strong privacy rights, there is no clear protection for people's digital identity after death. In a world where technology can now create almost perfect digital copies of people, this leaves the deceased open to misuse. Without a law to stop it, anyone could create a digital replica of a dead person and use it however they want.

On the other hand, countries like the United States (California) are already protecting the digital likeness of deceased people. For example, *California's Civil Code Section 3344.1*,[92] created by Assembly Bill 1836,[93] says that no one can use a dead person's name, image, or voice for business purposes without the family's or estate's permission. If someone does it anyway, they could be fined at least $10,000, and the law protects these rights for up to 70 years after death. In India, we do have the DPDPA,[94] but it does not go far enough. Yes, under Section 14(1),[95] a person can choose someone to handle their data after they pass away. But what if no one is nominated? The law gives no answer, leaving a big gap.

So, while Indian courts have been clear that privacy rights don't continue after death, it's clear that India now needs stronger laws to protect the digital lives and reputations of people who are no longer with us, especially as technology like deepfakes becomes more common.

[91] *Krishna Kishore Singh v Sarla A. Saraogi* 2021 DHC 1870.
[92] California Civil Code § 3344.1.
[93] California Assembly Bill 1836, 2023.
[94] Digital Personal Data Protection Act 2023 (India).
[95] Digital Personal Data Protection Act 2023 (India), s 14(1).

SUGGESTIONS

The Digital Personal Data Protection Act[96] in India faces several challenges in addressing the unauthorized creation and use of digital replicas of deceased individuals. While the Act offers a general framework for data protection, it lacks specific provisions for handling the unique ethical and legal complexities surrounding posthumous digital personas. To address these gaps, it is necessary to enhance the Act with more targeted regulations that address concerns around digital replicas.

A. Amend the Indian Succession Act to Recognize Digital Assets as Inheritable Property

The Indian Succession Act, 1925[97] needs to be updated to include digital assets-like a person's image, voice, and online presence, as property that can be passed down to family members. This change is important as in cases like that of Sushant Singh Rajput, where his father went to court to stop the unauthorized use of Sushant's name, image, and likeness in films and media. Since current laws don't fully protect a person's digital identity after they pass away, families have limited ways to protect their loved ones' digital legacy.[98]

By including digital assets in inheritance laws, families would have the legal right to control how these digital identities are used, allowing them to approve or block any use that doesn't align with their loved one's wishes. This would prevent misuse or exploitation of digital identities for profit, helping ensure that the person's memory is respected.

B. Proposal for Enhanced Protections of Digital Replicas of Deceased Data Principals

We suggest that the Digital Personal Data Protection Act[99] (DPDP Act) should clearly cover the digital replicas of people who have passed away under Section 10(1)(a) and (b).[100] Right now, the DPDP Act [101]mainly protects the personal data of living people. But with the rise of

[96] Digital Personal Data Protection Act 2023, Act No. 22 of 2023 (India).
[97] Indian Succession Act 1925, Act No. 39 of 1925.
[98] Arti Gupta, *'Personality Rights: Amitabh Bachchan, Sushant Singh, Anil Kapoor – Indian and Global Viewpoint'* (Bar & Bench, 6 January 2023) https://www.barandbench.com/law-firms/view-point/personality-rights-amitabh-bachchan-sushant-singh-anil-kapoor-indian-and-global-view-point accessed 27 October 2024.
[99] Digital Personal Data Protection Act 2023 (India).
[100] Digital Personal Data Protection Act 2023 (India), s 10(1)(a) and (b).
[101] Digital Personal Data Protection Act 2023 (India).

AI-generated digital replicas- such as avatars, deepfakes, and voice clones, there is a strong need to also protect the digital identity of those who are no longer alive. To show respect and safeguard the dignity of the deceased, their digital replicas should continue to be treated as "personal data" and should receive the same level of protection required from significant data fiduciaries. We recommend that this protection last for 70 years after the person's death.[102]

This is similar to California law (Section 3344.1 of the California Civil Code[103]), which protects a deceased person's name, voice, image, and likeness for 70 years after their passing. This period balances protecting the individual's memory with allowing for historical or cultural uses later. We also suggest that digital replicas should only lose this strong protection if they are fully anonymized. In other words, the replica should not be able to identify the deceased person in any way. This idea follows international data protection rules, like the GDPR[104], which only relaxes privacy rules when personal data is fully anonymized.

At present, Indian law does not clearly protect the digital identity of people after their death. This leaves space for misuse, such as using their likeness for commercial gain without consent. By updating the DPDP Act,[105] India can make sure that companies handling such sensitive data follow strict rules like obtaining consent from legal heirs and limiting how much data they collect and use. In short, this proposal will help India match international best practices and better protect the digital identities and legacies of people who are no longer with us.

C. Establishing a Digital Legacy Management Framework

The DPDP Act should establish a digital legacy management framework.[106] This would empower individuals to specify how their digital persona and data are managed after their death, similar to how will function for physical assets. Individuals could decide whether their digital identity is preserved, deleted, or passed on to heirs. Such a framework would prevent the unauthorized exploitation of posthumous digital replicas for commercial or harmful purposes and protect the digital footprint of deceased individuals from misuse. Cases like

[102] California Civil Code, s 3344.1.
[103] ibid.
[104] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
[105] Digital Personal Data Protection Act 2023 (India).
[106] Eduardo Akimitsu Yamauchi, Cristiano Maciel, Fabiana Freitas Mendes, Gustavo Seiji Ueda, and Vinicius Carvalho Pereira, 'Digital Legacy Management Systems: Theoretical, Systemic and User's Perspective' https://pdfs.semanticscholar.org/b41c/865db95bf1c84544e5e296c6a7778a178595.pdf accessed 28 October 2024.

Ajemian v. Yahoo! Inc. (2017),[107] where the family of a deceased man fights to gain access to his email account, highlight the legal challenges faced when managing the digital assets of deceased individuals. Without a clear legal framework, as seen in these cases, families navigate complex privacy laws, further emphasizing the need for provisions under the DPDP Act[108] to protect posthumous digital identities.

D. Extending Posthumous Rights for Digital Personas

India's Digital Personal Data Protection Act[109] (DPDP Act) can learn from California's Civil Code Section 3344.1(d),[110] which lays out clear rules for managing a deceased person's name, voice, image, or likeness. While Section 14(1) of the DPDP Act[111] allows individuals to choose someone to manage their personal data after they pass away, it doesn't say what should happen if no one is chosen. This is important because, with advancements in AI, it's now easier to create lifelike digital replicas of deceased people. California's law provides a solution by setting up a clear order for who gets control over a deceased person's likeness. If the person had a spouse, the rights go to them. If not, the rights go to the children or grandchildren. If there's no immediate family left, the rights pass to the parents.[112] This ensures that there's always someone legally authorized to manage the digital likeness of the deceased person. If the DPDP Act[113] included a similar system, it would make sure that the digital replicas and personal data of deceased individuals are handled by the right people. For instance, a celebrity's family could control how their likeness is used. Adopting such a clear system in India would protect digital identities after death and prevent misuse, just as California's law does.

E. Suggestions for New Rules under the DPDP Act for Managing Digital Estates of Deceased Individuals

The DPDP Act in India currently lacks clear provisions for managing digital estates posthumously. To regulate the management and inheritance of digital identities, India should notify Rules under DPDP Act[114] for Managing Digital Estate of Deceased Individuals. This

[107] *Ajemian v Yahoo!, Inc.*, 478 Mass 169, 84 NE 3d 766 (Mass 2017).
[108] Digital Personal Data Protection Act 2023 (India).
[109] ibid.
[110] California Civil Code, s 3344.1(d).
[111] Digital Personal Data Protection Act 2023 (India), s 14(1).
[112] California Assembly Bill No. 1836, Chapter 258 (2023–2024) https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1836 accessed 29 October 2024.
[113] Digital Personal Data Protection Act 2023 (India).
[114] Ibid.

rule must provide clear legal guidelines for how digital personas including social media accounts, digital avatars, online content, and personal data are handled after an individual's death. By drawing inspiration from California's inheritance laws, this would ensure that digital legacies are respected and protected, just as physical assets are managed through a will. This framework would empower individuals to decide how their digital identity is treated after death, aligning their digital legacies with their real-world wishes.

Firstly, the Digital Estate Rule should mandate explicit consent during an individual's lifetime regarding how their digital likeness and related personal data are used posthumously. Just as individuals choose organ donation preferences, they should be able to clearly state how their digital persona should be handled after their death. For example, an individual might choose whether their social media profiles are memorialized, whether their digital likeness can be used in commercial ventures, or if their digital identity should be erased or inherited by family members. This provision would offer individuals greater control over how their digital selves are managed after death.

Secondly, the rule should introduce a centralized digital consent registry where individuals can specify the use of their digital likeness. This system would allow people to declare whether their digital avatars or online content can be used for commercial purposes, memorialization, or entertainment and marketing. Such a registry would ensure that individuals' posthumous digital rights are clearly recorded and easily accessible to their heirs and legal representatives. Importantly, this registry would provide a means for individuals to revise or revoke their consent during their lifetime, ensuring that they retain control over their digital identity up until their death.

Thirdly, to ensure the integrity of this process, a comprehensive technology system would be necessary to track and record consent, ensuring transparency and preventing unauthorized use. This system could operate similarly to how medical organizations track organ donation preferences, guaranteeing that no digital identity is used without the individual's explicit consent. The technology should allow individuals to specify how their digital likeness is used, ensuring that these instructions are followed after death.

Fourthly, the rule should address the inheritance of digital identities and their related data. This provision would ensure that the individual's digital persona is passed on according to their

wishes, preventing unauthorized individuals from exploiting or mismanaging their digital legacy. It would also provide a clear framework for heirs, ensuring that they can manage the deceased's digital presence ethically and in line with the deceased's preferences.

The introduction of these rules under the DPDP Act for managing the digital estates of deceased individuals would create a comprehensive framework for respecting and protecting digital legacies. By empowering individuals to make decisions about their digital identities, ensuring explicit consent, and establishing inheritance guidelines, the DPDP Act can safeguard the posthumous rights of individuals in the digital realm.

CONCLUSION

The ability to create digital replicas of deceased individuals using AI is both exciting and concerning. While it offers families a way to remember and feel close to loved ones who have passed away, it also raises serious questions about consent, privacy, and misuse. India's Digital Personal Data Protection Act[115] (DPDPA) is a good start in protecting personal data, but it doesn't fully address what happens to our digital identities after we die. This paper has highlighted these gaps and suggested practical solutions to create a stronger legal framework. The main gaps in the DPDPA[116] include the lack of clear rules for digital rights after death, no provisions for inheriting digital assets if no nomination made under section 14(1) of DPDPA,[117] and no specific guidelines for managing digital replicas. For example, the Act doesn't say who controls a deceased person's digital identity or how to stop misuse like deepfakes or unauthorized commercial use. Court cases in India, such as *Deepa Jayakumar v. A. L. Vijay*[118] and *Krishna Kishore Singh v. Sarla A. Saraogi*,[119] have shown that posthumous rights aren't recognized under current laws, leaving digital identities open to exploitation.

To fix these gaps, this paper has proposed several recommendations. First, update the Indian Succession Act to include digital assets like social media accounts, digital likenesses, and online content as property that can be inherited. This would give families legal control over

[115] Digital Personal Data Protection Act 2023 (India).
[116] Digital Personal Data Protection Act 2023 (India).
[117] Digital Personal Data Protection Act 2023 (India), s 14(1).
[118] Deepa Jayakumar v A L Vijay & Others [2020] 1 CTC 670 (Madras HC)
[119] *Krishna Kishore Singh v Sarla A. Saraogi* 2021 DHC 1870.

their loved ones' digital legacies. Second, the DPDPA[120] should clearly protect digital replicas, requiring consent from families and setting rules for ethical use. Third, create a Digital Legacy Management System so people can decide how their digital identities are handled after death, like a digital will. Fourth, give families the right to access, correct, or delete digital data of the deceased. Fifth, introduce ethical rules to ensure digital replicas are used responsibly. Sixth, regulate cross-border data transfers to stop misuse in countries with weaker laws. Finally, add specific Rules under the DPDPA[121] manage digital estates, including a system for recording consent and ensuring transparency. These changes would have a big impact. Families would have more control over their loved ones' digital footprints, preventing misuse and ensuring their wishes are respected. Tech companies would have clear guidelines to follow, encouraging responsible innovation. India could also set a global example for managing digital identities ethically, helping other countries facing similar challenges.

However, some might argue that these rules could slow down innovation or be hard to implement. While these concerns are valid, the proposed framework balances regulation with flexibility. Clear guidelines would actually help tech companies by reducing legal uncertainties. Challenges like setting up a digital consent registry or enforcing cross-border rules can be tackled through phased implementation, public awareness campaigns, and international cooperation.

In the end, the goal is simple: to ensure that our digital identities are treated with the same respect as our physical ones. By updating the DPDP Act[122] and creating a strong legal framework, India can protect people's dignity, honour their wishes, and prevent misuse of their digital selves. As technology continues to evolve, these steps will help create a future where innovation and ethics go hand in hand. In a world where our digital lives outlast us, it's crucial to ensure they are treated with care and respect.

[120] Digital Personal Data Protection Act 2023 (India).
[121] ibid.
[122] ibid.

GUARDIANS OF PRIVACY: EVALUATING MENSTRUAL APP COMPLIANCE WITH US AND INDIAN MEDICAL LAWS

— *Joshua Joseph*[*]

ABSTRACT

With the recent rise health apps due to Covid Pandemic many users have become more health conscious as time went on. However, majority of these app users are still unaware of the possible breaches of data they may face from sharing such sensitive personal information with these applications. In the paper the author focuses on examining the regulatory frameworks in the US (HIPPA) and India concerning health app data especially that of menstrual tracking apps. Due to the nature of the data being collected, i.e., sensitive personal data, the author will conduct an analysis of popular health apps' privacy policies. The analysis is done by comparing them with the recently introduced Digital Personal Data Protection Act 2023 and trying to see if they adhere to the criteria made by the Act.

The paper also delves into the privacy policies of three specific apps: Flo, Eve by Glow, and the Apple Cycle Tracking App. These apps are known to be popular among women to track their menstrual cycle. However, some of them are known to have cases of data breaches which lead class actions suits being filed. Additionally, the paper would also include a table in order for the reader to further understand how these apps have drafted their privacy policy which does not properly inform the users regarding on what data is collected, stored and transferred. Finally , the paper will try to propose recommendations to address privacy concerns and raise awareness among users and policymakers in the constantly evolving medical technology landscape.

[*] The author is a student at Jindal Global Law School, O.P. Jindal Global University (JGLS).

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite." – Marlon Brando[1]

I. INTRODUCTION

The above-given quote by the Godfather himself is an important principle that has to be applied by the laws regarding privacy. In today's digital age, the use of applications also known as "apps" on our electronic devices has become a daily part of our lives. Different apps exist that solve our specific needs whenever we need to order an item or be reminded of a particular task. We are even willing to share private information about ourselves to things to create more convenience for us. We are no strangers to the fact that nothing is free, and if the item given to us is free, there is always a catch to it. More than 4.3 billion users use the search engine Google out of 7.9 billion people worldwide.[2] Even though it allows its users to explore and gain new information for free, it uses the data collected on the user to showcase ads to make revenue. Some have even considered that we are the products, and that Google uses us to sell information to companies who wish to expand their customer base. However, it is known that only general data is collected by Google, apps on the other hand collect more of a specific form of data leading to consumers worrying about their privacy. There have also been multiple cases in which these apps are listening in on the user when they are talking. This then is used to suggest any products that the user wants in the form of ads. This has also given rise to specific risks in apps that look into the fitness and health of their users.

The recent rise in popularity of health consciousness has also led to the market being flooded with wearable tech and related apps. This can be due to the result of Covid Pandemic as many individuals became health conscious during that period (See Fig 1 Below). These apps are designed to help users track their health and fitness goals. They collect data on parameters like heart rate, blood pressure, and sleep patterns to provide insights into overall health and well-being.[3] While these apps can potentially revolutionize healthcare, they pose a significant threat to user privacy as health apps have no strict regulations regarding collecting and using personal data. Many apps use tracking identifiers and cookies to track user activities on mobile devices,

[1] 'A Quote by Marlon Brando' (*GOODREADS*) <https://www.goodreads.com/quotes/433493-privacy-is-not-something-that-i-m-merely-entitled-to-it-s> accessed 8 March 2024

[2] 'How Many People Use Google in 2024? (Users Statistics)' (*WP Dev Shed*) <https://wpdevshed.com/how-many-people-use-google/.> accessed 15 March 2024

[3] Naithani P, 'Protecting Healthcare Privacy: Analysis of Data Protection Developments in India' (2024) 9 Indian Journal of Medical Ethics 149

and some of these applications use tracking across different platforms. It was discovered in research about two-thirds would collect advertising identifiers or cookies, one-third would collect a user's email address, and about a quarter could identify the mobile phone tower to which a user's device was connected, potentially providing information on the user's location.[4] In a recent research made by BMJ, it is stated that such apps have an "unprecedented risk to consumers' privacy," as 79 per cent of the apps that were reviewed were found to share user data in ways that violate the user's privacy.[5]

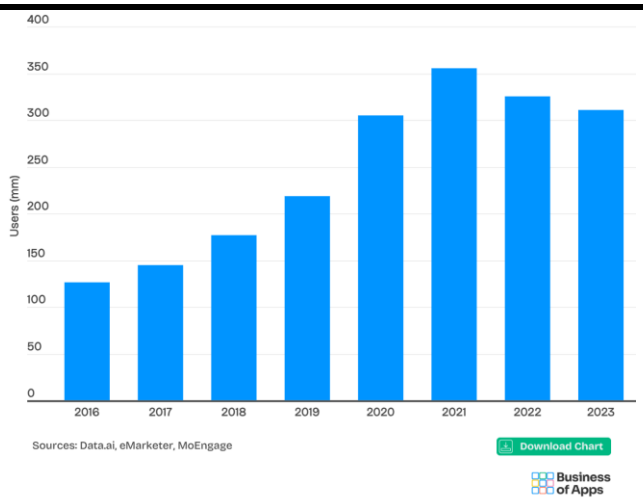


Fig 1. Surge of Users in 2020 and 2021

Source: Business of Apps

This raises serious concerns about the protection of personal data and the need for regulatory frameworks to safeguard user privacy. The lack of regulations in this area poses a significant challenge as it creates a situation where companies can collect and use personal data without any oversight. This is particularly concerning when it comes to sensitive health information. Users need to have confidence that their data is being handled with care and that it is not being used for any other purpose than what they have agreed to. This study, through an analysis of applications as examples aims to analyse data and privacy regulations of health apps in the US and India. It will evaluate their effectiveness in protecting personal information and identify gaps and challenges. The findings can inform better regulatory frameworks and promote trust in the industry.

[4]'Nine out of 10 Health Apps Harvest User Data, Global Study Shows' (*The Guardian*, 17 June 2021) <https://www.theguardian.com/technology/2021/jun/17/nine-out-of-10-health-apps-harvest-user-data-global-study-shows> accessed 8 March 2024

[5] Grundy Q and others, 'Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis' [2019] BMJ l920

The paper is divided into three parts; the first section will investigate the current system in the US and India. The second section will analyse popular health apps and conduct a privacy policy analysis regarding them. This includes applications such as period trackers which are known to take sensitive data about a woman's menstrual cycle that may be used to profit the company itself. Additionally, in this section, the author will also examine the efficacy of the current legislative framework against the conduct/practices of the applications. The third and last section will provide already existing recommendations to create awareness among users and policy drafters to tackle the new age of technology in the medical sector that mines user data.

II. THE MEDICAL SYSTEM

According to the World Health Organisation (WHO), digital health encompasses eHealth (including mHealth) and emerging areas such as big data, genomics, and artificial intelligence. This also broadens the scope of healthcare beyond traditional clinical settings.[6] WHO highlights how digital health empowers individuals to manage their health and wellness through self-monitoring tools, educational resources, and decision-support systems. This patient-centric approach can lead to earlier detection of health issues, improved medication adherence, and ultimately, better health outcomes. Additionally, digital health facilitates the collection and analysis of vast amounts of healthcare data, enabling researchers to identify trends, develop targeted interventions, and personalize treatment plans. This data-driven approach holds immense potential for advancing preventive care, optimizing resource allocation within the healthcare system, and ultimately, transforming the way we deliver healthcare globally.

A. The US System

In the US the Health Information Portability and Accountability Act (HIPAA) safeguards all Protected Health Information (PHI) held by covered entities. The act is known to impose heavy fines and penalties on healthcare organizations that fail to protect patient medical information properly.[7] However, it is first important to know what all are included in the definition of health information. As per (§160.103) Administrative Simplification Regulations, health information is defined as any information, including genetic information, whether oral or recorded in any

[6] 'WHO recommendations on digital interventions for health system strengthening' (*WHO*, 2019) <https://iris.who.int/bitstream/handle/10665/70474/1/WHO_RHR_10.19_eng.pdf> accessed 10 March 2024

[7] 'HIPAA Violation Fines' (*THE HIPPA JOURNAL*) <https://www.hipaajournal.com/hipaa-violation-fines/>accessed 11 March 2024

form or medium, that *"Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."*[8] The definition itself encompasses a wide range of information as it includes sensitive information about the health of the patient but also their payment plans and financial information (including insurance).

Furthermore, PHI is further defined as "*individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.*"[9] This includes names, phone numbers, email addresses, Medicare Beneficiary Numbers, biometric identifiers, x-rays, scans, physician's notes, diagnoses, treatments, eligibility approvals, claims, and remittances. Therefore, if any such information about a patient existed it would be either in a digital format or a physical format.

The Act applies to all healthcare facilities, healthcare providers, and other healthcare parties (insurance and billing companies) that transmit PHI electronically. These businesses are referred to as "covered entities." The HIPAA requirements also extend to the relationships between covered entities and their vendors especially those that handle PHI or other sensitive data.

However, an important distinction must be made between the following.

i. apps made by healthcare facilities (under a covered entity)
ii. apps for fitness, diet etc (applications that are not by a covered entity or a business associate of a covered entity)

The Department of Health and Human Services (HHS) provided that for such apps to not come under the ambit of the HIPPA, they should be a direct consumer-based product wherein the developers have no relation to any covered entity. Furthermore, the data in an app by a covered entity, the data is stored for its purpose, while an app not associated with a covered entity is only saving data for the consumer. Furthermore, the HIPAA Breach Notification Rule was implemented in 2009 to ensure that non-HIPPA entities would be held liable if there was a

[8] 'What Is Considered Phi under HIPAA? 2024 Update' (*The HIPAA Journal*) <https://www.hipaajournal.com/considered-phi-hipaa/> accessed 8 March 2024
[9] *Id.*

breach in maintaining the personal health records (PHRs) of its consumers. PHRs include any information that is related to the care of a patient and is maintained by the patient.

B. The Indian System

The current system for regulating digital health in India is nascent. As per the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002 (1.3 Maintenance of Medical Records), the data regarding the patient should be retained for 3 years and computerized for quick retrieval. However, due to digital advancements in the medical sector, many amendments have come forth to deal with the digitalization of patient information.

In February 2020, the Ministry of Health and Family Welfare released two notifications concerning medical devices in India. The first notification expanded the definition of "drugs" under the Drugs and Cosmetics Act, to also include "medical devices." Such devices included implant devices and software that is intended to assist human/ animal body diagnosis, prevention, monitoring etc. The Second Notification amended the Medical Devices Rule 2021 regarding the registration of such medical devices before the Drugs Controller General of India, and such devices had to be registered before 1st October 2021.

The addition of software in the definition of "drugs" in the Drugs and Cosmetics Act seems to be problematic as it targets any software that "*assists a human body in diagnosis, prevention, monitoring or supporting life.*" Such a definition would also include health apps that monitor a person's diet, heart rate, food habits etc. However, such health and wellness apps often lack the same level of rigour in data collection and security compared to medical devices used in clinical settings. This broad definition creates a regulatory grey area, making it unclear which apps require registration and how stringently they need to comply with data privacy regulations.

An important piece of information that is to be noted is that the government did make some progress in defining health data in 2018 and how organizations can retain and use information. The Ministry of Health & Family Welfare brought this up in the draft of the Digital Information Security in Healthcare Act (DISHA). "Digital Health Data" is defined in Section 3(e) as an electronic record of health-related information on a person's (i) physical or mental health; (ii)

information about any health services they may have received.[10] Additionally, the corporation is mentioned as an entity under Section 3(f), which holds it accountable for any violations of the act's sections. This demonstrated that India would have had a law pertaining to medical data similar to the HIPPA, but it appears that the Bill never was enacted due to the Data Protection Act being drafted around the same time, so the possibility of clashing was more likely between both the laws.

i. Health Data under DPDPA

The Digital Personal Data Protection Act, 2023 (DPDPA) doesn't directly address health apps, but its broad definition of "personal data" likely applies to the information they collect, including health information. The Act, however, does not create a stricter category for "sensitive personal data" that includes health data, requiring stricter user consent and limitations on how this data is processed. While specific regulations for health apps are absent, the DPDPA likely mandates clear user consent, limits data collection to the app's purpose, minimizes the amount of data collected, and requires security measures to protect sensitive health information. The following terms will be used in the privacy policy review:

Data Principle- refers to the person to whom the personal data relates. This includes; (i) a kid, comprising the child's parents or legal guardian; (ii) an individual with a handicap, comprising the guardian acting in their place.[11]

Data Fiduciary- An entity or organization handling personal data is called a data fiduciary. They acquire information and are in charge of gathering, storing, processing, or disseminating it. Name, address, phone number, and much more can be included in this info. Additionally, data fiduciaries are essential in guaranteeing that customer data is safeguarded and handled appropriately.[12]

III. PRIVACY POLICY ANALYSIS

As stated before, the use of health apps has blown up in recent years due to the convenience they give its users. Period-tracking apps have become increasingly popular among women,

[10] (*MINISTRY OF HEALTH & FAMILY WELFARE,*) <https://main.mohfw.gov.in/sites/default/files/R_4179_1521627488625_0.pdf,> accessed 16 March 2024

[11] Digital Personal Data Protection Act, 2023 § 2 (k) , No. 113, Acts of Parliament, 2023 (India).
[12] Digital Personal Data Protection Act, 2023 § 2 (l) , No. 113, Acts of Parliament, 2023 (India).

enabling them to monitor their menstrual cycles, predict ovulation, and provide various health-related information. These apps offer several features and functionalities, such as cycle analyses, personalised health support, and notifications about ovulation cycles. Some apps also provide suggestions on hormonal imbalances, irregular cycles, and lifestyle changes based on the symptoms reported by users. These apps have advanced beyond standalone applications, with one provider offering period tracking solutions through a texting service. However, these apps have recently faced criticism regarding their data collection practices and privacy issues. Therefore, the following apps were looked into during the research, it is to be noted that this is a small sample size of all current apps that are found:

A. Flo

Flo is a widely used tracking app with over 350 million users for ovulation and period tracking, fertility calendars, and pregnancy assistance. Its office is located in England. The app is also ISO/IEC 27001 certified which means that it meets the international standard of practices and principles that manage risks related to the security of data owned or handled by the company. In the summary of its privacy policy, it states to have an Anonymous Mode option which allows the user to use the app without inputting any data regarding themselves. The app states that it is GDPR compliant. It is to be noted that the current analysis is based on the privacy policy that is effective from October 31, 2023.

B. Eve by Glow

Eve by Glow is a period tracker and sex app for women "*who want to take control of their health and sex lives.*" The app is one of four that provides services especially for women the other being more in line towards period tracking. The app predicts the user's next period and their chances of pregnancy. It also tracks their moods and symptoms to discover trends in their cycles. The privacy policy given by the website is a general policy for all of the 4 apps and so does not contain a specific policy for its menstrual tracking app. In the author's opinion, it is best not to impose a general privacy policy for apps that have different uses as it may lead to a clash in the definitions, or give the company the benefit to collect data that is not for its legitimate use. It is to be noted that the current review is of the policy that is effective from June 17, 2023.

C. Cycle Tracking By Apple

This is an inbuilt menstrual tracking section made by Apple in its Health App. As per the general policy Apple has made for all its health wear, the major aspect it looks into is the user's privacy. Apple has been one of the companies that has boasted to put its customer's privacy first. Furthermore, one of the claims made by the company was that the data had been collected from the user, which was then anonymised and successfully used to further research women's health.

	Flo	Eve by Glow	Apple (inbuilt Menstrual Tracker)
Consent	**Not Upto Standard**	**Not Upto Standard**	**Good**
Data Collection	**Not Upto Standard**	**Not Upto Standard**	**Fair**
Data Processing	**Not Upto Standard**	**Not Upto Standard**	**Good**
Data Retention	**Fair**	**Fair**	**Good**
Third Parties	**!**	**!**	**Fair**
T&C	**Not Upto Standard**	**Not Upto Standard**	**Not upto standard**
Unique Features	**Fair**	**Fair**	**Good**
US, UK	**Fair**	**Fair**	**Fair**

The following image shows a colour-coded version of the following assessment made, the varying colors signify the threat in each of the categories:

Terms used in table

"**Good**" – The app has good measures in place

"**Fair**" - The app has fair measures in place

"**Not Upto standard**" - The app does not have proper measures in place

"**!**" – The app does not at all have proper measures in place

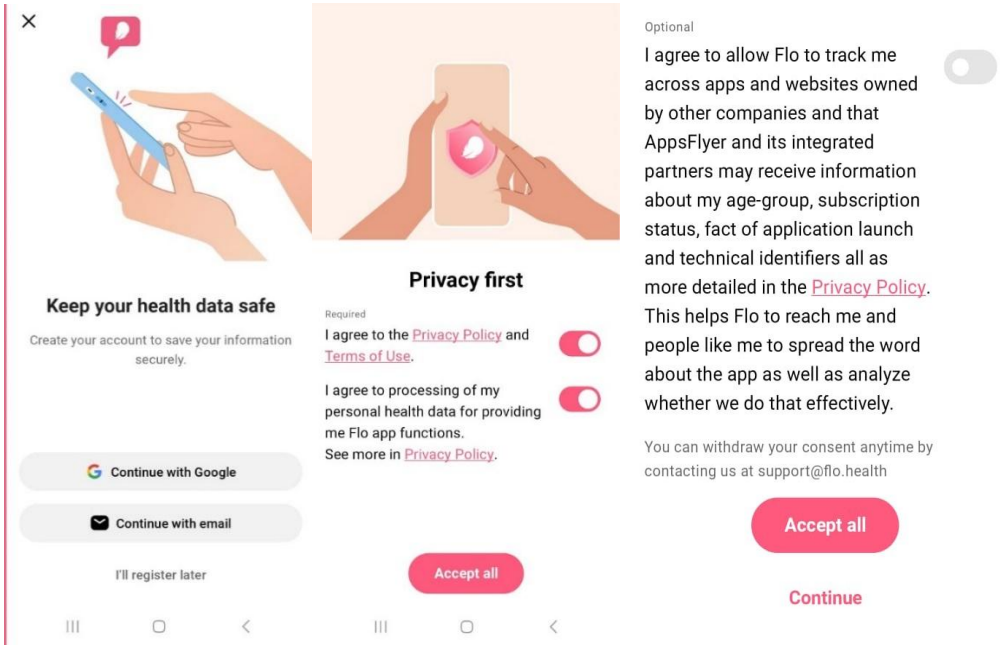
D. Review of the Apps

i. How the particular application takes the consent of the user and it is as per the law stated under the DPDPA

Under Section 6 of the DPDPA, the consent given should be *free, specific, informed, unconditional and unambiguous with clear affirmative action*. It will also signify an agreement to the processing of the Data Principal's data for the specified purpose and be limited to such personal data as is necessary for such specified purpose. However, it seems that the Act also included the act of deemed consent as the Data fiduciary can process the principal's data for legitimate purposes without their explicit consent.

- *Flo*

When the Flo Account was created, the user consent seemed to be bundled and did not explicitly state what information about them was being collected. This undermines the consent given by the Data Principle. Due to the nature of the data being collected, it is even harder for the Data Principle to know what is being collected about them.



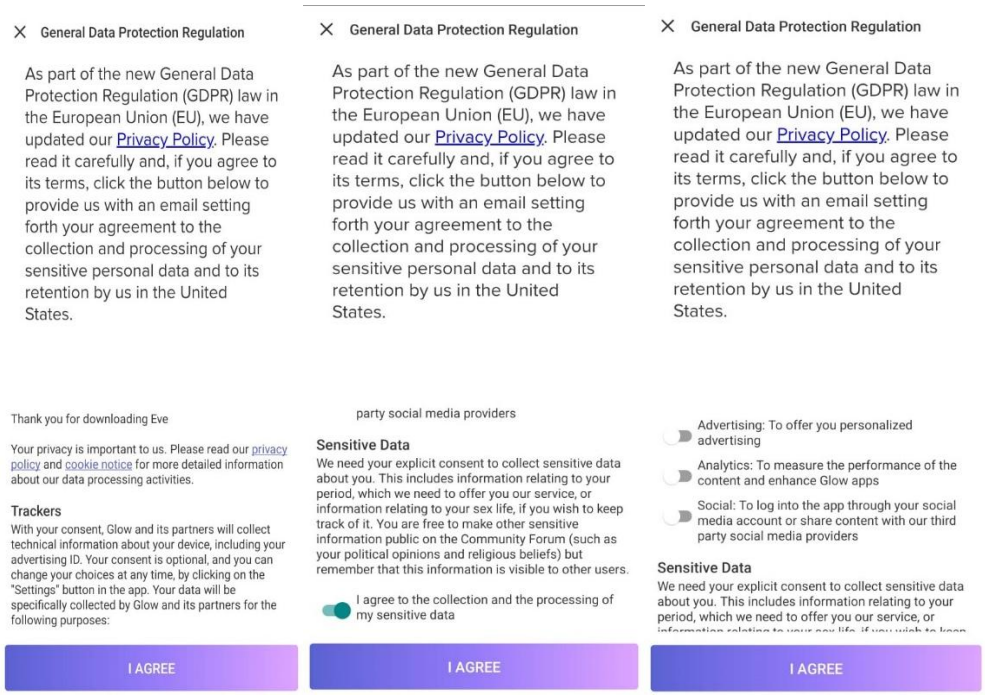
Source: Flo (Android)

Additionally, the policy offers the user the option to opt out of receiving mail. This is presented as giving the user "the freedom" to choose whether they want to unsubscribe from emails.

However, in the author's opinion, it would be better to make the procedure more of an opt-in format, as it gives the user control to select how they want their data to be processed.

- *Eve by Glow*

In the case of Eve, consent is taken during the creation of the account. During this, the app clearly stated that it is compliant with the GDPR. The following images showcase how the user is given an array of options regarding the use of the data being collected. This set of options clearly informs the user of the intended use of the data being collected. However, the user is not fully informed of what "sensitive data" is being taken and does not state the identity of the other "Partners" that Glow has while initially tracking the user. If such information was given then it would have led to the Data Principal being more informed of their decisions.



Source: Eve by Glow (Android)

- *Apple*

The Cycle tracker is part of the Health App by Apple, due to it being all part of one app, the user is notified about what all data is being taken of theirs for the purposes of the period tracking. However, as the app is part of the Health App the Data Principal has to input more data regarding their menstrual cycle.

ii. Data collected from the user by the application (and if there is a legitimate purpose) and whether the data collected is prohibited.

- *Flo*

Sensitive Data- The app also collects more sensitive data, including information regarding your weight, height, body mass index (BMI), body temperature, menstrual cycle dates, pregnancy, other symptoms relating to your health, and even details about the user's physical and mental well-being, including their sex life. However, Flo does put forward a table in which it shows what data is collected and for what purpose.

Data Regarding Children- The app claims to not collect any data with a child who is less than 13 years of age. However, it has only given the exception in the jurisdiction of England, which only allows children above the age of 16 to use the app. This is seen to be compliant under the DPDPA as no minor's information is being taken.

Data Retention- According to Flo's policy, personal information will be kept for as long as is required to complete tasks or meet collection needs. While complete erasure from backup systems may take up to 90 days, users can request and deactivate their accounts as well as have their data erased. Data erasure is normally done within 30 days. When an account is cancelled, data is usually lost and cannot be recovered. When an app is deleted or an account is inactive, personal data is stored for three years in case it is needed for future activation or installation. Retention may also be required for changes to app functionality. Even with efforts to anonymize data, some personal information might need to be kept after an account is closed to fulfil legal requirements, settle disagreements, or carry out contractual commitments.

- *Eve by Glow*

Sensitive Data -The app collects various sensitive data, including physical characteristics, health-related details like fertility and medications, and information on sexual orientation, pregnancy, and menstrual activity. It also tracks online activity and may combine user data with information from social media accounts.

Data Regarding Children- Regarding children, the app gathers data like name, date of birth, physical attributes, photos, and health information, potentially violating regulations on data collection from minors. This is one of the main issues with Glow as it has given a general policy for all of its health apps and so it seems to be a violation of data gathering of minors, this itself is a violation of Section 9 of the DPDPA and does not mention any alternative way in which it states that its making measures to ensure the safety of the data of the user's child. Therefore, it seems that there is a possible violation of Section 9 (3) which states that the Data Fiduciary cannot collect data on tracking/ behavioral monitoring of the minor.

Data Retention- Data retention is determined by legal requirements, with options for deletion, anonymization, or isolation of personal information when it's no longer needed.

- *Apple*

Sensitive Data- As per its policy data regarding the user is collected from all Apple products that the user has and is synced with iCloud. Therefore, if the user has items like the Apple watch and the iPhone, the data regarding them will be collected as long as it is consented to.

Data Regarding Children- The health policy does not have a specific provision regarding minor's data, however, due to Apple being under California Law it cannot collect data regarding minors.

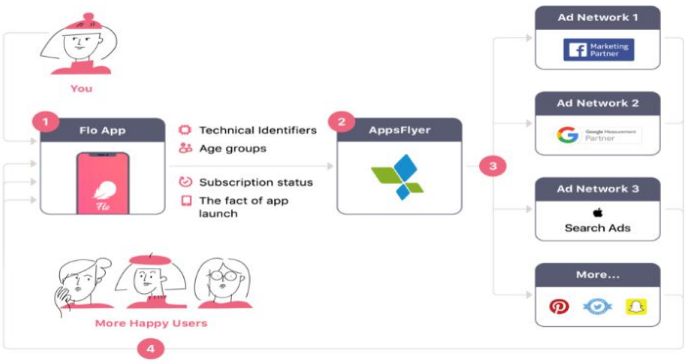
Data Retention- the policy states that the users can review, edit, and delete their Health app data at any time. This gives the user great autonomy over their own sensitive personal data and does not require days to be executed

iii. Data Processing and used by the application, and whether the data is transferred out of India and if it given to unknown third parties.

- *Flo*

The following image is taken from the Flo privacy policy and it clearly states that the user's data would be given to a third party named AppsFlyer which is a private mobile marketing analytics and attribution platform. This platform then further claims to protect the data of the

user while sharing the data with other platforms, while also ensuring its safety. Furthermore, the Privacy policy has properly put forward a few third-party companies it uses aid from to help process the data, however, it is clear that it is not all of them and so can be questioned the other third-party companies that have access to the data.



Source: Flo

- *Eve by Glow*

Their privacy policy outlines sharing data with lots of third-party advertisers, service providers, business partners, and professional advisors. The app also claims to use the user's data for its purpose for research and development purposes, including to analyze and improve their "Service." However, during such activity, it states that it first anonymizes the data to remove any part of the data that can identify the individual. Furthermore, it is noted that the app does give the Data principal the option to connect their social media accounts to the app to monitor the user's "mental health," however, it can be used for other purposes and so is questionable.

- *Apple*

With regards to the Cycle Tracking Health App, apple is seen to be ahead of the other two apps as does not share any information with third parties, unless it is consented to by the user themselves. This also includes other persons and even medical institutions who wish to access the individual's data.

iv. The Terms and Conditions of the App

- *Flo*

The terms of use state that it is an agreement that is a legally binding contract between the user and Flo Health UK Limited. Further states that it is not liable for any misinformation that the user received due to typographical error/ translation error. The app also cautions the user stating that it cannot and does not guarantee health-related improvements or outcomes. This seems to be a general contractual agreement between the Data Principle and Flo.

- *Eve by Glow*

Under the terms of use, it is stated that Eve does not provide any medical advice to the users. Furthermore, the terms and conditions signify an agreement between the user and the company and if the user does not want the company to take any of their data, they should stop using the service. Further, it is stated in the terms that Glow is the sole owner of all information it collects.

- *Apple*

The terms of use given by Apple are general ones as states are seen as general agreements between the company and the user.

v. Other Jurisdictions such as the California Act and EU GDPR would deal with how differently it is applied compared to the Indian/ International version

- *Flo*

Flo is approved to transfer personal data from the EU and Switzerland to the US under the EU-US Data Privacy Framework and the Swiss-US Data Privacy Framework (DPF). The user can mail complaints about the gathering and use of data to dpo@flo.health. Unresolved complaints may be brought to arbitration by following the procedures specified in the policy. Additionally, customers in the US have the option to refuse to share their data with partners for analytics and advertising. Personal data that is deemed sensitive is only utilized when absolutely necessary. Users have the right to inquire about the personal data that is gathered about them, how it is used, and whether or not it is shared with outside parties for the purpose of direct marketing.

- *Eve by Glow*

According to the US citizen policy, the corporation offers users outside of California the opportunity to opt out of the policy's requirements. The policy specifically lists the Data Protection Officer in the EU section, who should be notified in the event of any concerns. It also specifies in full the user's rights, the legal foundations for processing, and the channels for filing complaints with data protection authorities. It also addresses GDPR's standards for cross-border data transfers, making sure that transfers to nations outside of the EEA/UK are adequately protected.

- *Apple*

As per the main privacy policy, Apple especially states that different Apple-affiliated companies will be dealing with the data. Furthermore, Apple's international transfer of personal data collected in participating Asia-Pacific Economic Cooperation (APEC) countries abides by Privacy rules such as the APEC Cross-Border Privacy Rules (CBPR) System and Privacy Recognition for Processors (PRP).

vi. Cases against FLO

There have been many class action suits against Flo for its privacy issue. In 2021 a class action suit was filed against Flo for sharing intimate health data with its third parties in Florida. The transfer was accused of breaching users' privacy by revealing sensitive information to third parties through software development kits (SDKs). The complaint also claimed that although the other defendants "knew that the data collected and received from Flo Health included intimate health data," they did not take action because the information was "vital to their business," including for data analytics and marketing.[13]

vii. Cases Against Glow

In 2020 the California courts reached a settlement with the Glow company regarding "*serious privacy and basic security failures*," that put its users' "*sensitive personal and medical information at risk.*" In addition to a $250,000 civil penalty, the settlement contains injunctive provisions requiring Glow to follow state consumer protection and privacy laws, as well as an

[13] Mereken S, 'Fertility App Maker Flo Health Faces Consolidated Privacy Lawsuit | Reuters' (*Fertility app maker Flo Health faces consolidated privacy lawsuit*) <https://www.reuters.com/legal/litigation/fertility-app-maker-flo-health-faces-consolidated-privacy-lawsuit-2021-09-03/> accessed 16 April 2024

injunctive requirement requiring Glow to evaluate how privacy or security breaches may disproportionately affect women.[14]

IV. RECOMMENDATIONS

A. Constitutional Lens

Violation of Article 21 by private parties: In the landmark judgment of *K.S. Puttaswamy vs Union Of India*,[15] it was unequivocally recognized that privacy was a fundamental right, underscoring that *"Dignity cannot exist without privacy. Both reside within the inalienable values of life, liberty, and freedom which the Constitution has recognized. Privacy is the ultimate expression of the sanctity of the individual."*[16] This judgment established that the right to privacy under Article 21 is akin to a common law and a fundamental right.[17] Furthermore, it was held by the majority that fundamental rights under Articles 19 and 21 can be enforced against persons other than the State or its instrumentalities, including private entities. This broad interpretation suggests that violations of privacy by private companies could lead to infringements of the fundamental rights of users, thereby necessitating state intervention to protect individuals from such infringements. Furthermore, the case of *Kaushal Kishore vs the State of Uttar Pradesh,*[18] upheld the applicability of fundamental rights in the context of actions by private entities, indicating a judicial inclination towards ensuring the protection of FRs beyond the traditional state versus the individual. Therefore, the consumers can have a constitutional argument of privacy against any data breach/ illegal data collection that has affected them due to the irresponsibility of the Data Fiduciary.

***Application of absolute or strict liability*:** The concept of absolute or strict liability is often applied in cases related to Environmental Law and Public interest. Absolute liability is imposed on entities involved in hazardous activities, holding them absolutely liable for any harm caused. On the other hand, strict liability holds companies responsible for their offences but allows for certain defences such as an act of God or consent of the victim to absolve the defendant from

[14] 'Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information' (*State of California - Department of Justice - Office of the Attorney General*, 21 September 2020) <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93> accessed 25 April 2024
[15] (2017) 10 SCC 1.
[16] *Id.*
[17] INDIA CONST. art. 21.
[18] *Kaushal Kishore vs. State of Uttar Pradesh & Ors.,* (2023) 4 SCC 1.

liability. In contrast, absolute liability admits no exceptions, making the perpetrator unequivocally responsible for any damage caused, providing a higher degree of protection to victims of industrial hazards.

Traditionally, strict liability is not applied to data breaches, but the legal framework, particularly the Information Technology Act, 2000 (IT Act) and its amendments, outline responsibilities and penalties for entities failing to implement reasonable security practices, resulting in wrongful loss or gain (Sections 43A, 66C, and 72A). However, we can see that the Puttaswamy judgment and subsequent discussions on data protection laws emphasize holding entities accountable for breaches, stressing the importance of immediate notification to authorities in case of data breaches and indicating a move towards stricter compliance and accountability standards.

Application of government ID for private service: In an article by the *Indian Express*, it was stated that the government wished to promote the use of government ID when individuals use any private service,[19] This brought about some concerns about using such IDs in accounts like Facebook and WhatsApp. However, according to a government official, it is unlikely that social media platforms will enable Aadhaar-based authentication since they are built around anonymous use. Similarly, it can be also argued that for such apps the use of government Identification is not required due to the nature of data that is being collected about the individual.

B. Consumer Lens

Transparency and Consent: The best practice for ensuring user understanding and explicit consent involves the continuous communication of data collection and processing practices to users. This can be achieved through the implementation of a consent manager, which will help users understand the type of consent required for the app and facilitate the withdrawal process. Furthermore, a streamlined consent withdrawal system should be put in place to enable users to easily withdraw their consent at any time. This proactive approach would not only empower users, but also build trust between the company and the consumer. This would in the end benefit the menstrual app companies.

[19] Barik S, 'Wider Ambit for Aadhaar: Centre Wants PVT Entities, States to Use It for Authentication' (*The Indian Express*, 21 April 2023) <https://indianexpress.com/article/business/economy/wider-ambit-for-aadhaar-centre-wants-pvt-entities-states-to-use-it-for-authentication-8567794/> accessed 15 April 2024

Privacy-Friendly Policies: To enhance user understanding, companies can introduce privacy-friendly policies that are easily accessible and comprehensible. This can be achieved through the use of colour-coding or by providing a summarized version of the privacy policy and data collection practices.[20] Additionally, translating the privacy policy into local languages or utilizing audio/video methods can further improve accessibility, especially in regions with diverse linguistic backgrounds. By making privacy policies more user-friendly and easily understandable, companies can bridge the gap for users who may not be as technologically literate.

User Notifications, Updates and Security: The apps should also give a notice to the user similar to that of the HIPPA and constantly notify the user of any such update and consent if the purpose of the data being used/collected has been changed. This gives the consumer of the app more control over their data and so would lead to better results for both the company and the consumer.

Moreover, audits involving sensitive data collection should include privacy checks. This guarantees that the proportionality and legitimacy requirements are applied to data processing operations carried out by both public and private entities. These need to be the fundamental factors that privacy auditors should take into account when auditing data.[21]

Introduction of an Anonymous/ Incognito mode: Similar to what was given in Flo, there should be a where the data taken from the user is minimised. This is done by only collecting information that is solely needed for the function app and the user would be given an anonymized ID. Such a mode should be affordable and ensure the maximum amount of security for the user to ensure. Giving such an option ensures the users are given a choice to have control over their data and strengthen the efforts of data protection from the side of the data fiduciary. *Generational Rights*: The DPDPA, Section 14 grants a Data Principal the right to nominate another individual to exercise their rights in case of death or incapacity. It is essential to have

[20] Gupta, Indranath & Naithani, Paarth, 2022. "Transparent communication under Article 12 of the GDPR: Advocating a standardised approach for universal understandability," *Journal of Data Protection & Privacy*, Henry Stewart Publications, vol. 5(2), pages 149-161, August.

[21] 'Right to Privacy: Recognising Data Protection as a Fundamental Right' (*PWC*, June 2020) <https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/right-to-privacy-recognising-data-protection-as-a-fundamental-right.pdf> accessed 16 April 2024

a mechanism in place for notifying the company of such nominations to ensure a smooth process for rectification, modification, or erasure of data without dispute.[22]

In the case of applications like Eve, which specifically collects information about babies for health monitoring, concerns arise regarding minor users who never interacted with the app. This is because the app Glow retains specific data about them without the required consent. To address this, the company should acknowledge the collection of such data and share a list of the information they have with the government. Additionally, consumers should be informed if their loved ones' data is included in the database. The company should also ensure the *destruction* of such data if asked by the consumer as it is highly sensitive.

C. Regulatory

***Clear Definition of Health Data**:* To tackle the current issue using regulatory methods, the government can create a proper definition of private sensitive data or health data. This can be introduced under a set of rules that can regulate the health app industry. Such rules would hold the companies liable as many of them in the terms and conditions claim to not give any medical advice leading to consumers not being able to claim any compensation under the Medical Act. Furthermore, the type of data that is being collected itself is of a sensitive nature that can harm the user if it gets leaked.

***Fine System**:* One of the main methods of ensuring companies take the utmost care of the user's data can be the imposition of large fines that lead to compliance of the companies it can be similar to the antitrust fines of 2% of world earnings/ x amount, whichever is higher. This would naturally make the companies more risk-aversive and promote data minimisation and transparency. This may lead to companies not wanting their applications installed in particular regions, due to the potential fine that can be imposed on them. However, this can be that such a practice is done in countries in the EU and others like the US and it has not deterred any companies from operating in that jurisdiction.

[22] Digital Personal Data Protection Act, 2023 § 14 , No. 113, Acts of Parliament, 2023 (India).

Awareness Initiative: According to a study by IAPP,[23] approximately 68% of customers worldwide are very concerned about their internet privacy. This concern influences how much people trust businesses, organisations, and governments to gather, store, and use their personal information. However, in many cases, users are not aware of their rights regarding data. Therefore, users should be educated about their data privacy rights and given the ability to make informed decisions about sharing personal information with health-related apps. Strategies for raising user awareness, such as creating educational materials or interactive tools, running outreach efforts, and cooperating with consumer advocacy groups, should be implemented. Users should also be educated on the importance of consent in the internet era as it is different compared to consenting to a physical contract or document, as it is more instant and, in some cases, the user cannot understand the language given in the Privacy Policy/ Terms and Conditions.

In the instance of TikTok in the Dutch case, the DPA punished TikTok for failing to provide its users, many of whom are young children, with instructions for installing and using the app in English, making it difficult to grasp. TikTok's failure to produce a privacy statement in Dutch prevented them from adequately explaining how the app collects, processes, and uses personal data. This is a violation of privacy regulation, which is based on the notion that people should always be informed about what is being done with their personal information. Therefore, even providing the information in the local languages may increase the user's trust in the apps and also lead to more transparency with the Data fiduciary.

V. CONCLUSION

In today's digital environment, where health applications are essential instruments for tracking and controlling well-being, the significance of protecting private personal data cannot be emphasized. The present study has conducted a thorough investigation of the subtleties of data privacy laws in the US and India, highlighting the differences and difficulties associated with safeguarding user data. By carefully analyzing well-known health applications like as Flo, Eve by Glow, and Apple's built-in period tracker, the research has found concerning trends, such as unclear consent processes and inadequate data security safeguards. These disclosures

[23] Fazlioglu M, 'IAPP Privacy and Consumer Trust Report – Executive Summary' (*IAPP Privacy and Consumer Trust Report – Executive Summary*, March 2023) <https://iapp.org/resources/article/privacy-and-consumer-trust-summary/.> accessed 15 April 2024

highlight the pressing need for all-encompassing regulatory frameworks that can reconcile the necessity of user privacy protection with innovative practices in the field of digital health.

Based on proven legal precedents and optimal methodologies, the document presents an array of tactical suggestions intended to address the recognized obstacles directly. It defends the protection of fundamental rights to privacy from a constitutional perspective and considers the possibility of applying stringent or absolute culpability in data breach situations. Strong methods for user permission and control, user-centric privacy policies, and more transparency are critical from a consumer perspective. Proactive steps are also suggested to reduce privacy threats and provide consumers more control over their data, such as the addition of anonymous or incognito modes.

To promote compliance among industry players, the paper advocates for the regulatory domain to develop precise definitions for health data, strict enforcement procedures, and coordinated awareness efforts. It emphasizes how crucial it is for nations to work together and coordinate across borders to successfully handle the worldwide problems brought on by data privacy in digital healthcare. We can navigate the complexities of the digital age while upholding fundamental rights and fostering trust within the healthcare ecosystem by carefully balancing innovation and privacy protection, encouraging collaboration among stakeholders, and providing users with knowledge and control.

MOVING TOWARDS AN ORWELLIAN STATE? EXAMINING THE CENTRAL INCLINATION OF THE DPDPA

— *Tanya Sara George*[*] *and Abhishek Sanjay*[*]

ABSTRACT

The enactment of the Digital Personal Data Protection Act (DPDPA) signifies a pivotal development in India's data governance framework, although it raises grave concerns regarding its implications for individual rights and civil liberties. This article undertakes a critical examination of the DPDPA, arguing that its provisions disproportionately empower the state to curtail liberties under the guise of national security and protection; A regime that runs at the risk of characterizing the state as Orwellian, i.e., a state of constant over-surveillance and unfettered access to personal data. The expansive authority conferred upon the central government, coupled with the compromised autonomy of the Data Protection Board, risks the foundational principles of accountability, oversight, and individual freedoms.

The analysis is structured in three parts. The first part examines the extensive powers conferred upon the central government, including the absence of adequate safeguards to prevent misuse, thereby challenging the very foundation of individual freedoms, and further critiques the lack of independence of the Data Protection Board, its susceptibility to state influence and its potential role in exacerbating surveillance mechanisms. The second part explores the practical ramifications of these provisions, drawing parallels with the misuse of sedition laws and prejudicial enforcement mechanisms, signifying their potential to contravene constitutional guarantees. The third part situates the DPDPA within the broader international context, comparing its

[*] The author is a student at Maharashtra National Law University, Mumbai (MNLU).
[*] The author is a student at NALSAR University of Law.

framework to global data protection standards and proposing alternative approaches that strike a balance between safeguarding individual rights and addressing legitimate state concerns. It concludes by advocating for comprehensive reforms to align India's data protection regime with internationally recognised norms, thereby ensuring a rights-oriented governance framework

I. INTRODUCTION

Personal data has, time and time again, been granted the highest modicum of protection, in domestic and global jurisprudence. However, the recent inception of the Digital Personal Data Protection Act ("DPDPA"), elicits thinking to the contrary. In the spirit of paternalistic protection, the Act challenges the traditional norm of data regulation by surpassing essential prerequisites of governance, creating a classic example of legislative overreach of the state's paternalistic role into areas reserved for fundamental individual freedoms.

This article contends that the DPDPA has been formulated in a manner conferring a wide propensity for the weaponisation of control and regulation, in the name of national security and protection. This establishes the question of whether these measures could potentially pave the way for the conception of an *Orwellian* state, wherein citizens are susceptible to constant surveillance and data gathering, and their civil liberties are subordinate to the state's unfettered access to personal data.

The authors answer this question in the positive, by presenting a critique of the DPDPA Act, substantiating its structural fallacies and real-world implications. *Firstly,* the authors draw light on flaws in the DPDPA concomitant to granting unbridled powers to the centre, which begs the question of whether this legislation would lead to the creation of an Orwellian state. This is done in a twofold approach where Part A elaborates on the criticisms of the broad powers conferred by the DPDPA Act, and Part B establishes a line of argument against the lack of independence for the Data Protection Board. *Secondly,* the authors emphasize the applicability of the criticized provisions in establishing real-world issues, such as the act's forging of an unrestricted model of sedition law and prejudiced policing. *Lastly,* the authors compare domestic law to international legislation in proposing alternate thresholds for governing data protection, which meet global data protection standards.

II. THE DPDPA'S UNBRIDLED POWERS FOR CENTRE

This section is articulated into two parts. The first part analyses the DPDPA in light of the excessive discretionary powers granted to the central government. The second part evaluates the Data Protection Board and analyses its provisions to portray their paradoxical working, contrary to firstly, the rule of law, and secondly, administrative law.

At the outset, a significant factor to consider here is the definition of personal data provided by Section 2(t).[1] As per this, personal data is "*any data about an individual who is identifiable by or in relation to such data*." This definition grants the authority in charge an over-extensive ambit on deciding what classifies as 'personal data.' The excessive definition granted to personal data takes away from the fundamental principle of legality; the law must be precise, predictable, and clear.[2] As will be elaborately explained below, the lack of application of the maximum certainty principle in this legislation confers considerable power to the authorities stated in the act, actively displaying the prospect of abuse.[3] Although proponents argue that the definition is worded expansively in the nature of protection, further analysis indicates that the lack of adherence to fundamental principles of law places the wide definition at risk of gross misuse, outweighing its seeming goodwill.

A. Part A

This danger rises when considering the prolixity of the DPDPA to grant more powers to the central government. The Act grants over 40 powers to the central government to utilize its authority[4]. Notably, despite the dearth of adequate law regarding personalized advertising, the DPDPA, via section 9(4),[5] still grants the central government the authority to prescribe exemptions from Section 9,[6] i.e., the regulation preventing the profiling of children for reasons towards 'legitimate aims.' This seems to have been drawn from the CJEU judgment in *Meta*

[1] The Digital Personal Data Protection Act, 2024, §2(t).
[2] Endicott T, 'The Impossibility of the Rule of Law' (1999) 19 Oxford Journal of Legal Studies <https://ora.ox.ac.uk/objects/uuid:13972247-b645-4283-a8c0-24f29e3823dd> accessed 9 January 2025.
[3] 'Policing Low-Level Disorder: Police Use of Section 5 of the Public Order Act 1986 | Office of Justice Programs' <https://www.ojp.gov/ncjrs/virtual-library/abstracts/policing-low-level-disorder-police-use-section-5-public-order-act> accessed 9 January 2025, 'Trespass and Protest: Policing Under the Criminal Justice and Public Order Act 1994 | Office of Justice Programs' <https://www.ojp.gov/ncjrs/virtual-library/abstracts/trespass-and-protest-policing-under-criminal-justice-and-public> accessed 9 January 2025.
[4] Raghavan M, 'Rulemaking for Data Protection: Implementing India's Digital Personal Data Protection Act, 2023' (*Indian Journal on Law of Technology*, 5 July 2024) <https://www.ijlt.in/post/rulemaking-for-data-protection-implementing-india-s-digital-personal-data-protection-act-2023> accessed 9 January 2025.
[5] The Digital Personal Data Protection Act, 2024, §9(4).
[6] The Digital Personal Data Protection Act, 2024, §9.

Platforms Inc. v. Bundeskartellamt.[7] The judgement clearly established that the use of personal data for government use would not need to qualify as a legitimate aim in the GDPR as it is not commercial use and is for a bigger benefit. However, this view failed to take into account the granting of any guidelines or the creation of a structure within which the government must use this authority but rather granted them an unfettered right. This unfettered right is now explicitly granted in the DPDPA. Under Section 17(2)(a),[8] the government holds the authority to exempt instrumentalities of the State from all the provisions of the DPDPA, in their entirety.

In addition, the government can also exempt certain startups and innovation firms from necessary legal obligations such as the overarching need for obtaining consent. Ironically, to grant this exemption to a startup, it is judged on whether it is a startup by criterion by the Central government[9]. Section 17(5)[10] also allows the government to, before the expiry of 5 years, declare that any provision of this law shall not apply to such data fiduciary or classes of data fiduciaries for such period as may be specified in the notification. This grants the government extreme discretionary powers in what fiduciaries must be exempted. Moreover, the law is silent on the time period of such exemption, indicating that such exemptions could potentially be left up to the whims and fancies of the government. As the exception to startups, which is what one can reasonably and optimistically assume the intent of Section 17(5) is, are already clearly delineated in the act, this raises questions on why there needs to be a subsequent section allowing for wider usage.

Further, as per Section 36,[11] the central government can, at any time, issue directions to the data fiduciary *to "furnish such information as it may call for."* Once again, the excessive uncertainty conferred by this law runs the risk of the void for vagueness principle.[12] In the present scenario, the section is kept brief with an extremely wide ambit of power. The government has the power to take any information, at any time, from any fiduciary without a regulatory ambit to guide its actions. Arguing on the premise *of Connally v General*

[7] *Meta Platforms and Others v Bundeskartellamt* C-251/21 (CJEU, 4 July 2023) [27].
[8] The Digital Personal Data Protection Act, 2024, §17(2)(a).
[9] The Digital Personal Data Protection Act, 2024, Explanation §17(3).
[10] The Digital Personal Data Protection Act, 2024, §17(5).
[11] The Digital Personal Data Protection Act, 2024, §36.
[12] Horder J, 'Ashworth's Principles of Criminal Law', *Ashworth's Principles of Criminal Law* (Oxford University Press) <https://www.oxfordlawtrove.com/display/10.1093/he/9780192897381.001.0001/he-9780192897381> accessed 9 January 2025.

Construction Co,[13] a statute that lies so vague that the common man has to guess its interpretation and applicability is violative of due process of law.

Furthermore, Section 37[14] of the act grants the central government to block access to information to the public upon reference of the board in cases of public interest. This is done with respect to not just data fiduciaries, but *any* intermediary as defined under the Information Technology Act[15]. While the act does place two thresholds for action to be taken under this section in the form of (a) the board has imposed penalties against such data fiduciaries on two or more prior occasions, and (b) the board has recommended a blockage, this is easily circumvented due to the widely excessive powers granted. As will be further explained in Part B, the board, in this picture, works as a subset of the central government, allowing them to position with the government in any case, facilitating the satisfaction of both thresholds.

As mentioned earlier, 'personal data' is proffered an extremely wide ambit vide the act, allowing the central government, by virtue of a multitude of sections, to hold undue power in governance without a mandate to control the exercise of such power, establishing an emphatic argument for voidness due to excessive discretionary powers. Justice Bhagwati in *Bachan Singh v. State of Punjab*[16] has directly established the premise that the rule of law, must, as a matter of principle, exclude arbitrariness. Ironically, via the aforementioned sections, it seems as though the DPDPA has forgotten this precedential mandate. Further, as stated by the Supreme Court in *Naraindas v. State of Madhya Pradesh*,[17] if power conferred by statute on any authority of the State is vagrant and unconfined and no standards or principles are laid down by the statute to guide and control the exercise of such power, the statute would be violative of the equality clause, because it would permit arbitrary and capricious exercise of power, which is the antithesis of equality before law.

The DPDPA, through a plethora of sections, allow for vagrant and unbounded powers granted to the central government against the fundamental Right to equality,[18] Privacy,[19] and access to

[13] *Connally v General Construction Co*, 1926.
[14] The Digital Personal Data Protection Act, 2024, §37.
[15] The Information Technology Act, 2000.
[16] *Bachan Singh v. State of Punjab*, AIR 1980 SC 898.
[17] *Naraindas v. State of Madhya Pradesh*, 1974 SCC (4) 788.
[18] The Constitution of India, 1950, Art.14.
[19] The Constitution of India, 1950, Art.21.

information.[20] Moreover, there are no standards or regulations laid down under the act for the proper exercise of this power, which allows it to be reasonably assumed that this power is left up to the satisfaction of the central government to decide when to observe and to what extent. Succinctly put, it seems that a plethora of provisions under the DPDPA reinforces the arbitrariness of the excessive discretionary power doctrine, which logically, must render them invalid.

B. Part B

This unbridled power granted to the state is further compounded by the overseeing of the Data Protection Board[21] ("DPB"). *Inter alia*, the board functions as a point of contact for individuals to manage, review, and withdraw the consent given by them in the collection of their data.[22] While this seems to be an accessible and transparent platform, the actual functioning of the board is paradoxical. Now, as already established, the central government wields the authority to collect personal data for legitimate aims and allows the exemption of any data fiduciaries from the restrictions placed on them not to do so. The corollary, then, must be that the boards act as independent bodies to ensure transparency and accountability. However, the board is merely a facet of the central government, blurring the lines of the rule of law and the separation doctrine.[23]

While the DPB was premised on the GDPR and the DPA,[24] which runs independently of the government, the Indian model significantly deviates from this. Unlike the former, the DPB has a limited mandate in regulating data breaches and calling for action and inquiries.[25] Consider section 19(2),[26] which states that the chairperson and the member of the board shall be appointed by the central government. As per Section 20,[27] their terms and conditions of appointment shall also be decided by the central government. Further, the law only requires one member to be a legal expert. The chairperson is vested with the right to empower any board member to oversee any of its proceedings. Now, as the board holds the power to conduct

[20] The Constitution of India, 1950, Art.19.
[21] The Digital Personal Data Protection Act, 2024, §2(c).
[22] The Digital Personal Data Protection Act, 2024, §6(7).
[23] Fairlie JA, 'The Separation of Powers' (1923) 21 Michigan Law Review 393 <https://www.jstor.org/stable/1277683> accessed 9 January 2025.
[24] 'Understanding India's New Data Protection Law' (*Carnegie Endowment for International Peace*) <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en> accessed 9 January 2025.
[25] The General Data Protection Act, 2016, §27, §28, and §51.
[26] The Digital Personal Data Protection Act, 2024, §19(2).
[27] The Digital Personal Data Protection Act, 2024, §20.

inquiries and issue penalties for non-compliance with the law, these proceedings have an inherent and tangible legality to them. Allowing such processes to be overseen by someone who is not well-versed in the law, erodes the principle of legality and the rule of law.[28]

The court in *K A. Abbas v. Union of India*[29] shows the clear stance of the judiciary in holding that the inherent purpose of an executive board must be to exercise the rationality of its own mind. The court, in the instant case, held that such a board cannot merely be circumvented or a façade to the powers of the government but must be established to make decisions independently. The implicit control of the central government in the working of the DPA strikes at the heart of its independence and impartiality.

This lack of independence and preponderance of bias towards the central government, as it can be rationally presumed since the DPA is controlled by the government, subsequently violates the principles of natural justice. These principles hold that the body overseeing procedures must be *impartial*[30] and *free from bias*.[31] As held in *Franklin v. Minister of Town and Country Planning,*[32] this rule holds that the person making decisions must come to his adjudication with an independent mind, without any inclination or bias towards one side or the other in the dispute[33]. In the present case, under Sections 19 and 20[34] of the DPDPA, the tenure, salary, and other conditions for the working of the members of the DPA are set out by the central government. This is a *prima facie* indication of the central government holding substantial sway in the actions taken by the board, contrary to the natural justice principle against bias.

This is further exacerbated by the absence of an independent appeals mechanism. Sections 19 and 20 of the Act[35] allow the central government to exercise control over the Data Protection Authority, including the appointment, tenure, and salaries of its members. In practice, this

[28] M P Jain & S N Jain, *Principles of Administrative Law*, (9th ed, LexisNexis 2017).
[29] *K A. Abbas v. Union of India*, 1971 AIR 481.
[30] Chinn S, 'The Meaning of Judicial Impartiality: An Examination of Supreme Court Confirmation Debates and Supreme Court Rulings on Racial Equality' (25 April 2019) <https://papers.ssrn.com/abstract=3378211> accessed 9 January 2025.
[31] Olowofoyeku AA, 'Bias and the Informed Observer: A Call for a Return to Gough' (2009) 68 The Cambridge Law Journal 388 <https://www.jstor.org/stable/40388808> accessed 9 January 2025, Bonham's Case, (1610) Jeejeebhoy v. Asst. Collector citation, 1965 AIR 1096, Meenglass Tea Estate v. Workmen, 1963 AIR 1719.
[32] *Franklin v. Minister of Town and Country Planning,* [1948] AC 87
[33] M P Jain & S N Jain, *Principles of Administrative Law*, (9th ed, LexisNexis 2017), Atrill S, 'Who Is the "Fair-Minded and Informed Observer"? Bias after Magill' (2003) 62 The Cambridge Law Journal 279 <https://www.jstor.org/stable/4508998> accessed 9 January 2025.
[34] The Digital Personal Data Protection Act, 2024, §19(2).
[35] The Digital Personal Data Protection Act, 2024, §19 and §20.

renders the government both the data controller and the arbiter of disputes related to data access and protection. The absence of an independent appeals mechanism is particularly troubling. It effectively allows the State to act as the adjudicating authority for disputes arising under the DPDP Act, violating basic principles of natural justice. An independent supervisory authority to regulate the disclosure and processing of personal data has been recognised in international jurisprudence as essential to prevent abuse of discretion.[36] For instance, in *Peck v. United Kingdom*,[37] the ECHR categorically held that compelling the disclosure of personal data without adequate safeguards is violative of Article 17. The DPDP Act's failure to incorporate such safeguards exposes individuals to significant risks of unlawful interference.

III. MOVING TOWARDS AN ORWELLIAN STATE?

This part of the article builds upon the Act's strong penchant for the centre and concerns itself primarily with Section 7 of the DPDPA,[38] elaborating on its proneness to misuse. As per this section, the government holds authority over the data for *inter alia "interests of sovereignty and integrity of India, security of the state, friendly relations with foreign states, [or] maintenance of public order."* These terms are, however, overbroad, and not properly defined. The aforementioned provisions of the DPDPA form an observable pattern in favouring the state. These patterns, however, have an entirely different set of stakes when confronted with issues of national and individual security[39]. This section argues that these provisions can be used by the government as an instrument in curtailing civil and fundamental liberties and engaging in over-surveillance mechanisms. Part A analyses the implications of the new governance regime by drawing a parallel to the law of sedition, and stifling of free speech. Part B argues that the new regime may lead to flawed mechanisms of enforcement in policing and surveillance.

[36] The Privacy Act 1985 (Canada) art 7, art 8 art 36; Personal Information Protection and Electronic Documents Act (PIPEDA 2000, s 20(1) (Canada); GDPR (n 21), art 80, art 86, art 94; Directive (EU) 2016/680 (n 23), art 45, 46 and 47; Constitution of the Republic of Croatia 2010, art 28-29.
[37] *Peck v United Kingdom* App no. 44647/98 (ECtHR, 28 January 2003) [57];
[38] The Digital Personal Data Protection Act, 2024, §7.
[39] Byron Tau, Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State, (Crown 2024).

A. Part A: Eroding Fundamental Liberties

The *Puttaswamy v. Union of India* judgment,[40] the locus classicus on the right to privacy[41] in India, establishes the necessity of a narrowly tailored framework for any restriction on this right. The judgment's three-prong test of 1) legality, 2) proportionality, and 3) necessity, *pari materia* to the test established by ICCPR,[42] demands that any discretion afforded to competent authorities must be specific in scope and its manner of exercise clearly outlined. The DPDP Act fails to meet this standard.

Section 7 of the DPDP Act[43] grants the government sweeping authority to access personal data for broadly worded purposes such as "security of the state" and "maintenance of public order." The lack of specificity in these terms creates significant room for arbitrary decision-making. This concern is far from theoretical. The sedition law has demonstrated how vague and expansive legal provisions are prone to misuse, with a report[44] indicating that 96% of sedition cases were filed after 2014, often targeting individuals critical of the government. The overbearing threat of arrest hanging over any Indian critic of the government or any of its practices on social media[45] further highlights how data is often misused by the Indian government as a means to fulfil political agendas. The DPDP Act, by empowering the state to access data under similar vague justifications, raises the same risk of abuse, particularly to stifle dissent.

Furthermore, Section 17 of the DPDPA[46] provides for an exemption of Data Processing when undertaken for the "prevention" of an offence. The notion of "prevention" of an offence inherently entails a pre-emptive action, often directed at activities or individuals that are not yet engaged in illegal conduct. This stands in stark contrast to the foundational principle of criminal law that an act constitutes an offence only when the impugned act has violated or

[40] *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors* Writ Petition (Civil) No.494 of 2012
[41] The Constitution of India, 1950, Art. 21.
[42] International Covenant on Civil and Political Rights (ICCPR) (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, Art 17(2) and Art. 19.
[43] The Digital Personal Data Protection Act, 2024, §7.
[44] Nivedita Saxena and Siddhartha Srivastava, "An Analysis of the Modern Offence of Sedition", Manupatra Online [23].
[45]Ellis-Petersen H and correspondent HE-PSA, 'Online Hate Campaign Targets Indian Streaming Stars' *The Guardian* (3 July 2020) <https://www.theguardian.com/world/2020/jul/03/online-hate-campaign-targets-indian-streaming-stars> accessed 9 January 2025.
[46] The Digital Personal Data Protection Act, 2024, §17.

amounts to an attempt to violate a law, under a defined statute are punishable.[47] Additionally, it has been categorically held by judgements[48] and reports[49] that one's consent is a prerequisite for the admissibility of electronics as evidence in criminal cases. Now, however, the insertion of the word "prevention" may effectively create a leeway for the government to legally impeach the Right to Self-incrimination[50] by accessing one's data regardless of their consent in the name of prevention, without being legally required to meet any regulatory criteria.

It becomes pertinent to note that the test is conjunctive, and the failure to meet one standard renders the law violative of both the *Puttaswamy* judgment and India's obligations under the ICCPR.[51] Therefore, even if it is argued that the DPDP pursues legitimate aims in as much as it concerns national security and public order, the very fact that it fails to meet the set standard of legality renders it unconstitutional. Consequently, the DPDP Act, paradoxically, does not merely fail to protect the right to privacy but actively erodes it.

B. Part B: An Agency of Misuse and Biased Policing

Through this section, the authors argue that the explicitly wide definitions granted by the DPDPA fall out of the pigeonholes of 'protection' and 'national security' when they are confronted with unregulated and unfiltered capacity to misuse of a vagrantly high magnitude. The author Tau[52] reveals that the usage of personal data in the US has regularly allowed the government to man-hunt individuals in areas that are known to house criminal activity and to find undocumented immigrants. This trend of abuse and pattern recognition to follow prejudicial notions by the government stands as a stark example of what might happen to government-surveilled India. China's example,[53] wherein the government is overtly known for selling the data of citizens on the black market in exchange for monetary considerations, is an additional standpoint on why there is a need to safeguard the state's usage of citizens' data.

[47] Hall, Jerome. "Criminal Attempt. A Study of Foundations of Criminal Liability." The Yale Law Journal 49.5 (1940): 789-840; The Indian Penal Code, 1860.
[48] *CBI v. Mahesh Kumar Sharma*, 2022 SCC OnLine Dis Crt (Del) 48.
[49] B N Stiktrishna Expert Commission, WHITE PAPER OF THE COMMITTEE OF EXPERTS ON A DATA PROTECTION FRAMEWORK FOR INDIA, 2018.
[50] The Constitution of India, 1950, Art. 22.
[51] International Covenant on Civil and Political Rights (ICCPR) (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, Art. 17(2).
[52] Byron Tau, Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State, (Crown 2024)
[53] Greenberg A, 'China's Surveillance State Is Selling Citizen Data as a Side Hustle' *Wired* <https://www.wired.com/story/chineses-surveillance-state-is-selling-citizens-data-as-a-side-hustle/> accessed 9 January 2025

Taking an example, this risk becomes extremely grave when considering the allegations of the domestic government using the Pegasus spyware to target journalists and activists and the subsequent complete refusal of the government to comply with investigative efforts.[54] The Human Rights Watch organization[55] has noted the growing trend for domestic authorities to prosecute politically charged cases using data from the Pegasus software, a clear instance highlighting how data is often manipulated at the hands of the government. Additionally, the usage of social media data to spy on citizens has also been increasingly reported.[56]

A present model adopted by various online platforms before allowing for their usage is the utilization of 'cookies'.[57] Thus, these platforms oft function on an 'allow or non-use' model concerning the usage of their platforms.[58] These cookies allow platforms to track individual movements along the internet and thereby create a digital profile based on one's data.[59] While this is concerning in itself on the grounds of violations of the Right to Privacy,[60] the DPDPA exacerbates this issue by allowing the state to have access to such information whenever they want, without the need for any guidelines or safeguards to regulate this usage.

Further, the government has already, in the past, via the Diksha app, paradoxically, an app formulated by the Indian Education Ministry for children, used the data of said children for purposes of targeted advertising[61]. Ironically, as per the act, children are the only class protected from their data being obtained by agencies freely. Furthermore, it has been proved time and time again that the usage of technological data in proffering civil or criminal liability

[54] Deep A, 'Pegasus Spyware Found on Indian Journalists' Phones after Apple Alert: Amnesty International' *The Hindu* (28 December 2023) <https://www.thehindu.com/news/national/pegasus-infection-found-on-indian-journalists-phones-after-apple-alert-amnesty-international/article67682427.ece> accessed 9 January 2025

[55] 'India: Dangerous Backsliding on Rights | Human Rights Watch' (13 January 2022) <https://www.hrw.org/news/2022/01/13/india-dangerous-backsliding-rights> accessed 9 January 2025

[56] Freedom House's "Freedom on the Net 2019" reported that governments are increasingly relying on social media to spy on their citizens.

[57] Cahn A and others, 'An Empirical Study of Web Cookies', *Proceedings of the 25th International Conference on World Wide Web* (International World Wide Web Conferences Steering Committee 2016) <https://dl.acm.org/doi/10.1145/2872427.2882991> accessed 9 January 2025

[58] Samriddhi, 'Throwing Free Consent under the Bus? : Situating the "Pay-or-Consent" Model in the Global South' (*The CCG Blog*, 30 October 2024) <https://ccgnludelhi.wordpress.com/2024/10/30/throwing-free-consent-under-the-bus-situating-the-pay-or-consent-model-in-the-global-south/> accessed 9 January 2025

[59] Gowda S, 'Cookies to Track Digital Consumer Behaviour' *The Times of India* <https://timesofindia.indiatimes.com/readersblog/different-types-of-cookies/cookies-to-track-digital-consumer-behaviour-54624/> accessed 9 January 2025.

[60] The Indian Constitution, 1950, Art. 21.

[61] 'India: Data Protection Bill Fosters State Surveillance | Human Rights Watch' (22 December 2022) <https://www.hrw.org/news/2022/12/23/india-data-protection-bill-fosters-state-surveillance> accessed 9 January 2025.

is prone to the biases of human coders or receivers.[62] The legally acknowledged and widespread usage of such models in a country criticised for prosecuting religious minorities militates against the freedom to exercise one's fundamental rights. In this manner, inadvertent biases in enforcement may make technological prowess especially stringent on one particular community, or area for any one of the widely broad clauses mentioned in the DPDPA.

Furthermore, with the insertion of "prevention," the technological policing power granted by the DPDPA can be construed as "predictive policing."[63] Predictive policing is defined as the use of algorithms to identify and prevent crime,[64] thereby bringing it under the ambit of "prevention," as mentioned in the DPDPA. The problem that arises, however, is that even at a local level, policing in India has often been observed to disproportionately target vulnerable communities.[65] The data on which policing resources may be deployed are based on who has historically been more policed, rather than being indicative of who is likely to commit a crime. Now, allowing for discretionary predictive policing would inevitably exacerbate this scenario of over-policing[66] on a much larger scale and establish the institution of a discretionary cycle of over-policing.[67] This equips the government with the power to use data to hold that certain groups are predisposed to crime, thereby justifying their over-regulation while curbing their civil liberties.[68]

IV. CROSS-JURISDICTIONAL PERSPECTIVE - A BETTER APPROACH?

While it is acknowledged that the solutions adopted in Europe or other jurisdictions may not seamlessly be transposed to the Indian context due to the distinct socio-economic realities,

---

[62] Naijibi A, 'Racial Discrimination in Face Recognition Technology – Science in the News' <https://sites.harvard.edu/sitn/2020/10/24/racial-discrimination-in-face-recognition-technology/> accessed 9 January 2025.

[63] Sorell, Tom. "Preventive policing, surveillance, and European counter-terrorism." Criminal Justice Ethics 30.1 (2011): 1-22.

[64] Ramachandran Murugeshan, 'Predictive Policing in India: Deterring Crime or Discriminating Minorities?' (*LSE Human Rights*, 16 April 2021) <https://blogs.lse.ac.uk/humanrights/2021/04/16/predictive-policing-in-india-deterring-crime-or-discriminating-minorities/> accessed 9 January 2025.

[65] Hansen EV& TB, 'Citizens and the State: Policing, Impunity, and the Rule of Law in India' (1 March 2024) <https://www.thehinducentre.com/incoming/citizens-and-the-state-policing-impunity-and-the-rule-of-law-in-india/article67887312.ece> accessed 9 January 2025.

[66] Richardson R, Schultz J and Crawford K, 'Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice' (13 February 2019) <https://papers.ssrn.com/abstract=3333423> accessed 9 January 2025.

[67] Marda V and Narayan S, 'Data in New Delhi's Predictive Policing System', *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2020) <https://dl.acm.org/doi/10.1145/3351095.3372865> accessed 9 January 2025.

[68] Heavan WD, 'Predictive Policing Algorithms Are Racist. They Need to Be Dismantled.' (*MIT Technology Review*) <https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/> accessed 9 January 2025.

borrowing from the best practices can not only strengthen the DPDPA but also position India as a competitive global market. As established earlier, one of the most severe shortcomings of the DPDPA is the lack of an autonomous body to oversee data protection.

Looking to the West, the General Data Protection Regulation (GDPR) in the European Union mandates the creation of independent supervisory authorities under Article 51.[69] These entities, such as the Irish Data Protection Commission (DPC)[70] and Germany's Federal Commissioner for Data Protection and Freedom of Information (BfDI),[71] ensure compliance through autonomous operation and accountability mechanisms. Similarly, the United Kingdom's Information Commissioner's Office (ICO), governed by the Data Protection Act 2018 (DPA 2018),[72] functions independently to enforce data protection standards across public and private sectors. In contrast, the DPDP Act vests significant discretion with the executive branch, potentially compromising the impartial enforcement of data protection laws. India could establish a similarly independent authority, empowered to monitor compliance, adjudicate grievances, and impose sanctions without government interference, thereby alleviating the earlier mentioned risks of misuse.

Furthermore, a comparative analysis reveals that international laws impose stringent conditions on state data processing. For instance, the GDPR's Article 6[73] strictly delineates lawful bases for processing data, including by public authorities, while Article 23 restricts derogations from data subject rights to situations that are "necessary and proportionate" and accompanied by specific safeguards. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) reinforces these principles under Section 5(3), which mandates that all data processing meet the test of reasonableness.[74] The DPDPA, however, provides broad exemptions for state actions under Section 17, risking arbitrary use of personal data. Limiting state discretion by requiring data processing to adhere to proportionality and necessity tests, as in the GDPR, or subjecting state actions to oversight by an independent authority, as in Canada, would strike a better balance between public interest and individual rights.

[69] General Data Protection Regulation, Art. 51 (EU).
[70] Data Protection Committee (Ireland).
[71] The Federal Commissioner for Data Protection and Freedom of Information (Germany).
[72] Data Protection Act (2018) (UK).
[73] General Data Protection Regulation, Art. 6 (EU).
[74] The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) §5(3).

The DPDPA remains largely silent on the Right to be Forgotten and any mention of it remains vaguely defined and lacks the procedural clarity necessary for its effective implementation. The GDPR sets a precedent under Article 17[75] by detailing specific grounds for erasure, such as when the data is no longer necessary for the purposes for which it was collected or when consent is withdrawn. The Srikrishna Committee Report similarly recommended a five-point framework for evaluating RTBF claims, including factors like the sensitivity of the data, the passage of time, and the purpose of data collection.[76] At the very least, the DPDP Act should incorporate the guidelines from the 2019 Bill, which allowed RTBF in circumstances such as the completion of the purpose for data collection or the withdrawal of consent.

V. CONCLUSION

The authors attempt to draw a line of argumentation that, paradoxically, the DPDPA erodes the very protection of data it seeks to emulate. The analysis indicates that the present framework creates a paradigm of centralized controls that outweighs its necessity. This extends to more than just theoretical conjecture and, if applied and utilized, portends a transcendent shift in the state-citizen relationship. Due to their application of misuse, the act creates a distinguishment of the state as paternalistic to Orwellian. This implication extends far beyond privacy concerns. As our analysis demonstrates, the Act's provisions could serve as instruments for the systematic curtailment of civil liberties, potentially facilitating the emergence of a surveillance state. This trajectory raises fundamental questions about the future of democratic governance in an increasingly digital India.

Looking forward, the challenge lies not merely in reforming specific provisions of the DPDPA, but in reconceptualizing the relationship between state power and individual rights in the digital age. This requires a framework that recognizes data protection not as a concession granted by the state, but as an inalienable right that requires institutional safeguards and meaningful limitations on government authority in an increasingly digital 21st century.

[75] General Data Protection Regulation, Art. 17 (EU).
[76] Srinivasulu, K., M. Channa Basavaiah, and D. Ravinder. "Srikrishna Committee: thorough but unviable." Economic and Political Weekly (2011): 16-18.; Singh, Ajay Pal, and Rahil Setia. "Right to Be Forgotten-Recognition, Legislation and Acceptance in International and Domestic Domain." Nirma ULJ 8 (2018): 37.

BEYOND THE CLICK: HOW THE DIGITAL PERSONAL DATA PROTECTION ACT TRANSFORMS ONLINE BOOKINGS

—Kumar Nishant[*]

ABSTRACT

The Digital Personal Data Protection (DPDP) Act, 2023 marks a significant step forward in India's efforts to protect digital privacy in an era dominated by data-driven technologies. This landmark legislation introduces a strong framework focused on consent, data minimization, and empowering users, with an emphasis on secure and transparent data practices. For online booking platforms, the Act addresses the major issues of excessive data collection, security risks, and misuse of personal information. It takes inspiration from international standards such as the GDPR, which highlights essential user rights such as the right to be forgotten, and enforces strict penalties for non-compliance. Despite the novel approach of the Act, implementing it is not without its challenges. The small and medium enterprises would be put to a strain financially, explicit consent requirements could add operational complexity, and public awareness about data privacy is still a major area that needs to be addressed. The Act does bring India more in line with global norms on privacy, thus being a facilitator of consumer trust and innovation along with balancing economic growth and individual privacy. The DPDP Act attempts to strike the right balance for data protection, bringing digital progress into alignment with the safeguards of privacy. The long-term rewards in terms of greater user trust, global alignment, and a secure digital environment are undeniable, but the effort will require major restructuring and investment along the road to compliance. Its success depends more on cooperation through lawmakers, businessmen, and

[*] The author is a student at Maharashtra National Law University, Aurangabad (MNLU).

users to ensure an easily implemented strict environment. Lastly, the DPDP Act forms the way toward securing a safer environment and promoting data protection and reiterating a fundamental right-in this case, privacy-that secures the very position of a global leader from India in international data protection governance.

I. INTRODUCTION

"*The impact of the digital age results in information on the internet being permanent. Humans forget, but the internet does not forget and does not let humans forget."*

-The Supreme Court of India in K.S. Puttaswamy v. UOI

In India's digitizing economy, the Digital Personal Data Protection Act, 2023 signifies a major milestone in the protection of personal data. For the first time, the Act critically examines long-standing practices of data collection, storage, processing, and disclosure by digital service providers. Among the most affected are online travel agencies like MakeMyTrip and Goibibo, as well as airline platforms such as Indigo and Air India. These are the core players in the modern travel industry, dealing with huge amounts of personal data that is essential for smooth online booking but also a significant threat to privacy. Online travel and hospitality sectors have evolved in recent years which ease the customers to books their reservations in flight, hotels and other services seamlessly. That ease though carries a cost. The platforms collect sensitive personal data in large quantities including names, addresses, contact information, payment details, and even government issued identities like Aadhaar, PAN, or passport numbers. While data gathering is an extremely important aspect of service provision but it puts people at great risk of unauthorized access, misuse, and hacking. Now India has become a prime target of encrypted cyberattacks and becomes second, only behind the US, for the highest recorded incidents across the globe at 5.2 billion, according to the Zscaler ThreatLabz 2024 Encrypted Attacks Report.

The risks associated with such data collection by the platforms can lead to breach of personal information which can be used further for hacking and illegal purposes. Event such as 2021 Air India breach incident where sensitive information of 4.5 million users, including passport

and payment details, were compromised[1] and such incidents not only reduce consumer confidence but also show that the existing legal framework does not hold much ground for addressing these shortcomings. The DPDP Act intends to bridge this lacuna with a legally sound as well as robust data protection framework inspired by international standards like the General Data Protection Regulation and inspired by India's deeply rooted constitutional values. Even in a broader sense, the Act recognizes privacy as a fundamental right, as emphasized in Puttaswamy's Case[2], covering both the broad and integral part of the right to life and personal liberty as enshrined in Article 21[3]. The DPDP Act operationalizes this principle through clear guidelines for data fiduciaries, users' empowerment, and strong penalties against violators.

II. FRAMEWORK FOR DATA PROTECTION: THE DPDP ACT'S CORE PROVISIONS

A. Protecting Privacy Through Explicit Consent

The DPDP Act makes explicit and informed consent an integral element of practices relating to data processing. As provided under Section 4[4], all data fiduciaries, that is, entities which collect and process data, must obtain consent from users before they will be able to collect or use their information. Such agreement should be informed, specific, and purpose-oriented, so users know beforehand exactly how their data will be used. Unlike erstwhile practices where the terms and conditions have not been clearly provided and have been so structured that users unknowingly grant broad permissions for data sharing, this Act, however, requires that the platforms indicate the reason why data are being collected. The provision prevents users from blanket permissions to access data which may in turn lead to its misuse.

"Informational Privacy is a facet of right to privacy"[5]. The concentration on consent is in point with the landmark judgment of K.S. Puttaswamy v. Union of India[6] where "Informational Privacy" has been considered as an essential part of personal liberty, requiring that any intrusion on the personal data of any individual be justified by a clear, informed consent. The provision requires online booking platforms to overhaul their consent mechanisms. For example, when a user makes a flight booking and the data is shared with third parties such as

[1] Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers, Forbes, Retrieved from (https://www.forbes.com/sites/carlypage/2021/05/23/air-india-data-breach-hackers-access-personal-details-of-45-million-customers/)
[2] AIR 2017 SC 4161
[3] Article 21, The Constitution of India, 1950
[4] Section 4, DPDP Act, 2023
[5] Ibid 2
[6] Ibid 2

travel insurers or hotel booking services, it must be fully disclosed to them and they must agree to that. Under such circumstances, failure to obtain the consent would attract huge penalties under DPDP Act.

B. Data Minimization And The End Of Over-Collection

Data minimization is another basic premise of the DPDP Act, which stipulates that collection of data should be confined to only the data necessary to achieve a given purpose. In other words, this corrects the major issue associated with the digital arena-one of over-collecting user data for purposes apart from that for which a service is provided. This principle means that online booking platforms can no longer collect superfluous information under the guise of improvement of services or for targeted marketing.[7] For example, although a platform may lawfully require a traveller's name, contact information, and payment details to complete a booking, collecting further data, such as a user's demographic profile, preferences, or social media handles, would probably contravene the DPDP Act principle of necessity. The narrower scope of collecting data reduces the risk of its breach but also encourages platforms to focus data processing activities and make them transparent. In turn, this should improve user trust because people know their personal information is not placed in unnecessary risk.

C. Security Obligations And Accountability Measures

There is an obligation imposed upon the Data Fiduciaries under Section 8 of the DPDP Act to guarantee the security and integrity of the personal data in their custody. These obligations range from the use of state-of-encryption to secure payment gateways and regular audits to find and remedy possible vulnerabilities. The Act also mandates organizations to establish mechanisms for the reporting and resolution of data breaches, which further reiterates accountability.[8] The thrust of data security is not new; it is supported by judicial pronouncements such as Google India Pvt. Ltd. v. Visakha Industries[9], where the Supreme Court emphasized the responsibility of intermediaries to prevent the misuse of user data. These obligations have been translated into law by DPDP Act, which now makes them mandatory, subject to penalties for noncompliance. It implies investment in solid cybersecurity infrastructure for online booking platforms. Such companies must also deploy advanced threat

[7] Goldsteen, A., Ezov, G., Shmelkin, Data minimization for GDPR compliance in machine learning models. AI Ethics 2, 477–491 (2022)
[8] Section 8, DPDP Act, 2023
[9] AIR 2020 SC 350

detection systems and have clear protocols for dealing with cases of data breaches. For instance, in the case of a cyberattack compromising user data, such platforms are under obligation to immediately notify both present and future users as well as relevant authorities, with action to contain such breach and prevent recurrence.

D. User Empowerment Through Rights Over Data

The right to be forgotten has been recognized in several judgments, such as Jorawar Singh Mundy v. Union of India[10] and the Puttaswamy's[11] case. It is implicit in the overarching framework of the right to privacy. One of the most transformative aspects of the DPDP Act is the recognition of individual rights over personal data. Users can get their data, rectify any errors, and request to have the data erased under Section 12[12] when the information is no longer required. The right to be forgotten, under this section, becomes an excellent means of maintaining the private life of a person in this era of technology. For instance, a tourist may request the erasure of travel information after completing a trip when they have booked a flight. Also, users can transfer data to another service provider, making it possible to have increased competition and choice in the market. This empowerment goes well with observations of the Apex Court in Puttaswamy's Case stating that permanence in digital information may infringe an individual's right to privacy and hence "Informational Privacy" is facet of right to privacy under article 21[13]. The DPDP Act empowers the individual with control over the duration of their data and who should have access to it. For online booking platforms, this would require significant changes in operations because these rights would necessitate a great deal of change in business operations. Companies will have to create systems that are user-friendly in processing requests for data access, correction, and deletion. These platforms will also have to revise their data retention policies for the fulfilment of the Act.

III. OBSTACLES AND OPPORTUNITIES

The DPDP Act, 2023 is a very important framework for data privacy and protection in India but poses serious challenges in its implementation. One of the biggest hindrances is that the costs involved in conformity to the Act shall be borne by businesses- mostly the small and medium-sized enterprises. These companies will have to spend on developing cybersecurity

[10] W.P. (C) 3918/ 2020 & CM APPL. 11767/ 2021
[11] Ibid 2
[12] Section 12, DPDP Act, 2023
[13] Ibid 3

infrastructure, management of data systems, and hiring Data Protection Officers to comply, which will not be effective on the cost front. Then there is the complexity of managing explicit and informed consent from users, especially in an industry where data is shared with a number of third parties, requiring sophisticated systems to obtain and manage consent effectively. Another great challenge has been the principle that one must ensure that data collection is limited while ensuring that the quality of service is not compromised thereby. The need for different forms of data security, on the other hand, complicates the issue too. Strong security protocols, including encryption as mandated by the Act, usually demand technical sophistication and are expensive for businesses that do not have allocated budgets. Furthermore, although the penalty system of the DPDP Act for violation recommendations is high, there remains a challenge of uniform compliance management across industries and enterprise sizes. The Data Protection Authority will have to be energized sufficiently to monitor compliance with its mandates.

Restrictions over the cross-border data transfer in the DPDP Act might also create complications for companies which are global, because they may need to adjust their data storage and transfer practices because of the regulatory requirements. This lack of widespread familiarity and comprehension about the new act, among businessmen as well as consumers, might work against effective execution.[14] Since most businesses do not understand their obligations and most consumers do not know their rights under the Act, this could pose as a potential threat to realizing the objects of the Act unless a more comprehensive training and public awareness programmes are mounted. The last point is that the success of the DPDP Act would depend on clear regulatory guidance and consistent enforcement by the DPA. Lack of clarity in the regulation may cause confusion among businesses and delay compliance. If the DPA is slow in issuing regulations or has a poor record of consistently enforcing the Act, then it is unclear how businesses are supposed to comply.

IV. LESSONS FOR INDIA FROM GLOBAL DATA PRIVACY FRAMEWORKS

Inspired from international frameworks such as GDPR and CCPA, the India DPDP Act 2023 is a milestone step toward stronger data privacy, but there are also some lessons India can take forward to improve its data protection regime. There are aspects of explicit, informed consent involved under both DPDP Act and GDPR, wherein the concern of data collection has to be

[14] Mitchell, Andrew & Mishra, Neha, (2019), Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute, Journal of International Economic Law

clearly explained to the consumer by business houses. India needs to ensure that consent is transparent rather than it being vague agreements. Unlike the CCPA, which allows users to opt out of data sales, the DPDP Act, like the GDPR, stresses proactive consent for all data processing. Another key lesson is data minimization. The GDPR and DPDP Act are strict in gathering only necessary data, thus reducing the risk of exposure. In contrast, the CCPA is flexible rather than placing an absolute limit on what kind of data can be gathered. India can further strengthen the law by providing specific, proper purposes for collecting and regularly revising them. Another valuable lesson is the focus of the GDPR on data security. Both the GDPR and DPDP Act require businesses to secure data and notify users in the case of breaches. India should implement stringent security measures, especially in high-risk sectors like online booking, including audits, encryption, and breach notification protocols.[15]

Under the enforcement of GDPR, Article 83(4)[16] lays down the penalties of fines of up to €10 million or 2% of the worldwide turnover for minor breaches. Similarly, Article 83(5)[17] provides the fines of up to €20 million or 4% of the worldwide turnover in case of grave infringements, hence discouraging violation. In July 2019, the UK's Information Commissioner's Office said it intends to fine Marriott International £99 million for violations of the General Data Protection Regulation as it related to a cyber-attack that compromised over 339 million guest records. Meanwhile, the Dutch Data Protection Authority fined Uber €290 million for illegally exporting the personal data of European taxi drivers to the United States. In 2018, the ICO fined British Airways £20 million for a data breach that exposed customer information, including credit card details and personal data of over 400,000 customers[18]. Such cases highlight the need to follow strong data protection regulations and to seek users' consent, which will offer an important lesson to India's online platforms. Some steps that India can use in order to avoid identical breaches and penalties under DPDP Act are imposing tight fines and consistent enforcement practices for businesses. The introduction of a DPA is a step in the right direction, and such an authority's efficiency lies in the consistent application of the law. The third is that India can draw much from the approach of GDPR toward cross-border data transfer and ensure that this DPDP Act falls in all international standards for global data transfers. This would create a strong position of India among the nations and facilitate lots of international

[15] Hemalatha G, Saikrupaa K, Comparative Analysis of GDPR and Digital Personal Data Protection Act, 2023, IJCRT, Volume 11, Issue 12 December 2023
[16] Article 83(4), GDPR
[17] Article 83(5), GDPR
[18] British Airways fined £20m over data breach, BBC, Retrieved from (https://www.bbc.com/news/technology-54568784)

trade. This would make the informed consent stronger, enhance the data minimization, provide robust security, and enforce stringent penalties to make India achieve a world-class data protection framework that ensures both innovation and consumer trust.

V. WAY FORWARD: A NEW STANDARD FOR DIGITAL PRIVACY

The effective implementation of the DPDP Act requires a lot of work on many fronts. One such area is the fact that businesses, and especially SMEs, should understand and comply with the Act. However, most SMEs cannot afford to train their employees extensively or hire legal and technical consultants. They could certainly use subsidized government-led initiatives and much more online accessible modules for such issues; however, smaller businesses have a challenge with compliance without having such kinds of targeted support. Equally relevant is user education, empowering the rights of access, correction, and data portability in a user's hands. Nonetheless, raising awareness among this teeming population of India-the least digitally literate population-is also the challenge. Campaigns need to be made inclusive by using regional languages and resources that can provide a wider understanding. Without the widespread awareness of these rights, many users will not have a chance to exercise these rights. Investment in cybersecurity infrastructure is another imperative.[19] The Act asks for adequate measures of security, but the high technologies and audit requirements are cost-prohibitive for smaller organizations. The gap can be bridged through incentives provided by the government in terms of tax breaks or grants. Building secure and transparent data management systems is integral but resource-intensive. Automated consent systems and monitoring user preferences are very capital intensive and require high technical competencies. There is also the risk that companies might take a superficial compliance route to defeat the Act. Such compliance calls for constant checks by the regulatory agencies.

Effective enforcement will primarily depend on the collaboration of proposed Data Protection Authority (DPA). The DPA would have to come up with clear guidelines for consistent implementations, but without sufficient resources and actual autonomy, such effectiveness becomes doubtful. If the DPA is either weak or underfunded, that could reduce the Act just to rhetoric alone; hence little real influence on people's data protection practices. Adaptation to global standards such as the GDPR ensures compatibility with international frameworks and,

[19] Siva Karthik Devineni, AI in Data Privacy and Security, International Journal of Artificial Intelligence & Machine Learning (IJAIML) Volume 3, Issue 1, Jan-June 2024, pp. 35-49

by extension, data transfer across borders. In this respect, however, it must be balanced with Indian realities about the digital ecosystem. Regular review of the Act, carried out in the open, can ensure relevance without disregard for domestic reality. Another critical aspect in this context is industry cooperation; but competing interests often defeat the purpose. Neutral platforms, whether government-led or industry-sponsored, would prove useful in sharing knowledge that does not infringe upon competitive interests. Fragmentation of compliance practices across sectors would work against the objectives of the Act. Penalties and compliance monitoring need to ensure a balance between accountability and support. While the high-value fines prevent violation, indispensable are the clear guidelines and enough time for adaptation from the act on businesses, particularly on smaller ones. An appropriate progressive approach toward developing an authentic compliance culture would make this act realize the promise in respect of protection to user data.

VI. CONCLUSION

The Digital Personal Data Protection Act, 2023 was a significant leap forward for India's digital journey. It balances the requirements of the digital economy with the individual privacy aspect and hence has provided a new benchmark for data protection. Tough provisions in the Act exist primarily for online platforms to break the norms to bring the business a step closer towards prioritizing users' rights and being transparent. Changes might be difficult in the short term, but over the long term, achievement for the business will include consumer confidence, less risk of breach, and keeping pace with global best practices, all making this mandatory at some point. The implementation of the principles of the DPDP Act will bring comfort to the future when ease and privacy coexist; such a digital ecosystem would thus be safer and more reliable for all stakeholders. This Act stands out as a significant stride in India's initiative to safeguard private data and maintain the right to privacy during the modern age of digitization. With rapid growth of online services, particularly in areas such as online booking, the DPDP Act creates a safer and more accountable digital environment. Business houses are held at very high standards of protection, and users are able to have more control over their personal information. This legislation is a new, harmonized measure of the law in the field of data protection that puts it in line with other global data protection frameworks, such as GDPR, and adds user-centred and transparent provisions with severe penalties for violations. The purpose of this act would only become a reality when adopted through the perpetual cooperation of lawmakers, business persons, and consumers into its implementation. The main problems of

implementation are financial investments in compliance, restructuring systems for data management, and the establishment of new frameworks on consent. However, the benefits that flow from compliance include consumer trust, competitive advantage, and alignment with international privacy standards, which create compelling business incentives to adopt the provisions of the Act and make India achieve a world-class data protection framework that ensures both innovation and consumer trust.

A COMPARATIVE STUDY OF THE LEGAL FRAMEWORKS RELATED TO DATA PROTECTION IN INDIA, THE U.S.A. & THE U.K.

—Vaishnavi P[*]

ABSTRACT

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge." - Bruce Schneier.

Data protection is very important for personal rights and state duties. This study compares data protection laws in India, the U.S., and the U.K., focusing on their methods and challenges. In August 2023, India passed the Digital Personal Data Protection Act, recognizing the Right to Privacy under Article 21. Challenges remain, including low public awareness, weak institutional frameworks, and enforcement issues that must balance regulation and innovation. Bruce Schneier compares data in the digital age to pollution, emphasizing its potential harm. It underlines that safety and privacy have become crucial tasks, similar to environmental concerns that need solid efforts, collective involvement, and more focus on the growth of a nation's economy in a sustainable way, on par with data protection.

The U.S. adopts a sectoral approach. The state of California, however, has a very pioneering set of legislation. However, within California, the interest in economics prevails over the right to privacy in most instances: witness the Cambridge Analytica saga. The UK data protection framework is holistic, based on transparency, consent, and accountability. The extraterritorial reach of the GDPR has altered global standards and new laws for India, for example, but large and medium companies face serious problems in complying.

Each jurisdiction has its pros and cons. India's evolving law aims to balance strict compliance with economic growth. The U.S. approach is

[*] The author is a student at Christ (Deemed to be University), Bengaluru.

flexible but fragmented, risking loopholes in enforcement. Conversely, the UK's GDPR model is enforceable, yet scaling it for different infrastructures and digital literacy is challenging.

The paper focuses on major data breaches and legal remedies. The Aadhaar leaks in India show that a stronger institutional framework is the need of the hour. In the U.S., a disjointed system limits privacy protection. In the UK, under GDPR, heavy fines have been imposed to encourage compliance.

Keywords: Data Protection, Digital Privacy, Comparative Analysis, Digital Personal Data Protection Act 2023, Data Breaches, Artificial Intelligence, Privacy Frameworks.

I. INTRODUCTION

Human beings yearn for democracy as a demand of time for their justice. However, democracy in the present era does not represent the best form of government. It constantly reports corruption in and out of the system and delays in the Justice delivery system from the Executive and the Judiciary. The reality is that the hunger for power, money politics, fake manifestos, and all such blind statements just to take people in hand are just damaging democracy.

In the present scenario, there is always a bias that has been created in the last moment in the elections, such with the use of most modern technologies so as to win the elections, which always happens and can be preferably seen in India and the US. In India, we have the parliamentary system, whereas, In the US, it is the president who heads the Government then when we take a look at the protection of Data protection, which is an inherent part of the Fundamental rights under Article 21 of the Constitution of India as after the famous *Justice K.S Puttaswamy and Ors. v. Union of India and Ors.*[1], which quite clearly states that it's an integral part of Part III of the Constitution of India and needs to be protected. However, as the laws and technologies rise in high flow, they cannot be protected.

These include some of the ones that deal with the US legal aspect concerning Fundamental rights and Data Protection where; in the US, we have laws such as The Children Online

[1] AIR 2017 SC 4161

Protection Act, The Health Insurance Portability and Accountability Act[2] referred to as HIPAA, and the fair and accurate Credit Transactions Act, which is referred as FACTA.

In the case of the UK, we have DPA 1984 (Data Protection Act), the principles under the same Act and the amendment Act and the principles. Thus, we can see that all the countries have been keenly protecting their citizens' data as it has become their sole responsibility. Therefore, in this paper, we will explore data protection and the laws and actions of respective countries toward protecting the Data.

International cooperation would be of significant importance on a global scale when dealing with the transborder problems of data protection.[3] Such an example would include the EU-U.S. Data Privacy Framework or efforts that can be taken as part of OECD Guidelines[4] on the Protection of Privacy and Transborder Flows of Personal Data. In India, too a growth in terms of engagement with international privacy standards can be observed, as well as adherence to the norms of Convention 108+.[5]

In addition, the proliferation of authoritarian regimes has created a new challenge in data protection. Some governments in various countries have used personal data to track and monitor citizens under the veil of national security or public order.[6] The widespread adoption of surveillance technologies and the Social Credit System by the government of China perfectly exemplifies how personal data can be leveraged to enforce conformity and suppress dissent (Mozur, 2018). This trend of increased global surveillance and data collection carries much potential danger to the freedom and privacy of the individual.

Thus, it is the case that personal data protection is a crucial aspect in terms of democratic development and respect for human rights. As I discuss and compare the data protection laws

[2] New Jersey Institute of Technology, 'Safeguarding Patient Privacy in Electronic Healthcare in the USA: The Legal View' https://researchwith.njit.edu/en/publications/safeguarding-patient-privacy-in-electronic-healthcare-in-the-usa-

[3] Securiti, 'Data Privacy Laws and Regulations Around the World' https://securiti.ai/privacy-laws/

[4] Dale Howell, 'Has GDPR Really Changed the Relationship Between Businesses and Their Data Subjects?' (2018) ITProhttps://www.itpro.com/data-processing/31901/has-gdpr-really-changed-the-relationship-between-businesses-and-their-data

[5] Securiti, 'Data Privacy Laws and Regulations Around the World' https://securiti.ai/privacy-laws/

[6] Eunsun Cho, 'The Social Credit System: Not Just Another Chinese Idiosyncrasy' (1 May 2020) Journal of Public and International Affairs https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy

of India, the United States, and the United Kingdom, it becomes apparent that although there are different ways and approaches adopted by these countries regarding these challenges, the bottom line remains the same: protecting personal data is critical to the safeguarding of individual rights and freedoms in the digital age.

As the paper progressively delves, it seeks to mark unique approaches, common challenges, and possible synergies in India, the U.S.A., and the U.K. data protection frameworks. Ultimately, insights are drawn toward crafting resilient, adaptive policies that balance individual privacy rights adequately vis-a-vis technological and economic changes.

II. A COMPARATIVE STUDY OF THE LEGAL FRAMEWORK RELATED TO DATA PROTECTION IN INDIA, U.S.A. & U.K.

A. In India

India's move toward robust data protection started by first acknowledging a growing need for personal data protection amid rapid digitalization. Growing data breaches and the growing concern for privacy at the international level led India to develop the Digital Personal Data Protection Act 2023 for an all-around legal framework for protecting personal data.

The current data protection legislation in India, as of now directly, is the Digital Personal Data Protection Act 2023; the rules accorded with the Act are in the making, and presently, to add on, 'India has made itself a robust legislation' giving prominent importance to the protection of the data of the individuals and heavily punishing the wrongdoers. The delay in the establishment of contact with the Act and rules has to be severely condemned as the only hope for the citizen in this regard is a robust and stringent Act and Rules that Govern and protect the privacy of each individual in all the important areas where people interact and share their data. Information and Technology Act 2000, The Credit Information Companies Act 2005, IT rules 2011. Among these, nearly one that deals with it is the IT Act 2000. In India, what we can see is the illiterate acts that are done by the people in and out, which in turn creates chaos and confusion and thus contribute to the breach of data as such, whereas, in the US and UK, they

rely on the contractual obligations[7] also from the internal security measures.[8] At the nascent stage of the date, the Ministry of Information and Technology and the National Association for Software and Service Companies (NASSCOM)[9] have set forth amendments in the years 2004 and 2008 that, in turn, cover data privacy. Even later, that did not come to light, but even the same had flows regarding the biometric.[10]

In the last 10 years, India has also seen some of the most significant data breaches of all time, including the Airline's data breach,[11] the data that was stolen from CAT applicants,[12] and many more. And lastly, the data breach of COVID times in almost all states in and around the main reason is the lack of adequate legislation like the US, which curbs and controls the data of their citizens very aptly and concurrently. Irrespective of all these, we can again see that the Directive Principles of State Policies also lay down on the Government that it has to make policies in such a manner that they have to Part III and Part III has to co-exist with Part IV so Part III was given the upper hand and has to been given higher protection. In India, the most

[7] Governed by Indian Contract Act, 1872, India Code. Non-EU states where data protection has not been found to be adequate, such as India rely on an alternative avenue and ad-hoc solutions to procure and continue business transactions. The European commission and the data protection commissioner have the power to endorse "model contracts" specific to the transferring countries circumstances as well as power to approve particular contracts or other arrangements that provide satisfactory safeguards.

[8] VinayakGodse, Building an ecosystem for cyber security and data protection in India. (https://www.dsci.in/sites/default/files/India-Building%20an%20New%20Ecosystem_Vinayak%20v4.pdf)Indian IT and ITES industry, an important player of the ecosystem, has gained significant experience in cyber security and data protection. In its bid to protect client data, which are processed by these companies as a part of outsourcing or providing of services to specific security requirements, the industry has gained significant skills in India and experience in this field. All Global Security Vendors have their presence in India; many of them source their research talent from India and have built research facilities in India. Recent DSCI-KPMG Survey, confirms the fact that Indian industry is catching up with the information security trends fast, confidently facing new age security challenges through the use of technology and leading practices. The survey also highlights that increased sensitization for protecting the personal information being processed here, is driving their privacy initiatives

[9] The National Association of Software and Services Companies (NASSCOM) is a trade association of IndianInformation Technology (IT) and Business Process Outsourcing (BPO) industry. Established in 1988, NASSCOM is a non-profit organisation. NASSCOM is a global trade body with over 1500 members, of which over 250 are companies from the United States, UK, EU, Japan and China. NASSCOM's member companies are in the business of software development, software services, software products, IT-enabled/BPO services and e-commerce. NASSCOM facilitates business and trade in software and services and encourages the advancement of research in software technology. It is registered under the Indian Societies Act, 1860. NASSCOM is headquartered in New Delhi, India, with regional offices in the cities of Mumbai, Chennai, Hyderabad, Bangalore, Pune, and Kolkata. See more on: http://www.nasscom.in/about-nasscom

[10] Peter Carey, DATA PROTECTION: A PRATICAL GUIDE TO UK AND EU LAW 25 (2009)

[11] https://www.theregister.com/2021/03/05/oh_sita_airline_it_provider/

[12] https://amlegals.com/the-data-breach-saga-cat-candidates-personal-data-exposed-on-the-dark-web/#:~:text=The%20compromised%20data%20included%20sensitive,percentile%20scores%20were%20also%20leaked.

dominant part of the Right to privacy[13] comes under Article 21[14], and it's the people's choice whether to disclose their information simultaneously after even the landmark judgment. The Fourth Pillar of Democracy in India, namely "Privacy" under the Digital Personal Data Protection Act 2023, which is regarded as a landmark legislation. It deals with an age-old concern: private violations.

The new legislation also has stringent provisions as well as high-security features since the data being collected is to be protected at all means and therefore for the protection of Article 21, which has become a significant part after the *Justice K.S Puttaswammy Judgement*.[15]

The DPDPA also sets up a "*Data Protection Board of India*," which will look after compliance, probe breaches, and impose penalties.[16] Such a board has been designed to be independent. This means the data protection norms will be kept in place with no interference by the government, much like how the EU provides supervisory authorities under the GDPR at both national and EU levels.

The regulations also classify personal data into different categories, namely sensitive personal data and critical personal data. Sensitive personal data would enjoy more protection and additional restrictions on its cross-border transfer, while the protection measures for critical personal data would be stricter with more significant restrictions on cross-border transfers.[17]

Thus, the Digital Personal Data Protection Act of 2023 will likely be a precedent for all future legislation on data protection in India, and the landscape of data protection in India will change dramatically. With all the problems in implementing such an austere set of measures, the intent is to establish a Data Protection Board for privacy rights.

[13] 'Right to Privacy' (Lets Learn Law) https://www.letslearnlaw.com/right-to-privacy/

[14] The Historic SC Verdict On Right To Privacy In Five Points. https://toistudent.timesofindia.indiatimes.com/news/top-news/the-historic-sc-verdict-on-right-to-privacy-in-five-points/23882.html

[15] AIR 2017 SC 4161

[16] Ministry of Electronics and Information Technology, Government of India. "Data Protection Board of India Overview."

[17] National Law Review. "Classification of Personal Data under the DPDPA."

B. In United States

The Sectoral approach was also the method through which data protection was historically undertaken in the United States. Such an approach has been concentrated in specific industries such as health care and finance. As the issue of data privacy grows in significance, state-specific legislation such as the CCPA and CPRA arises to cover loopholes not found in a broad federal data protection law.

The United States of America has enacted statutes based on necessity, and the statutes that establish the laws that prevail in the country are The Video Protection Act of 1988,[18] the Cable Television Consumer Protection and Competition Act of 1992,[19] and the Fair Credit Reporting Act[20] of 1992. These multi-dimensional laws constitute part of the American laissez-faire system that co-exists with diverse social perceptions, and free speech, too, has been guaranteed under the constitution.[21] Another very important one that exists in the case of America is The Privacy Act of 1974, the Computer Matching and Privacy Act (FTCA), The Health Insurance Portability and Accountability Act (HIPAA), and The Gramm-Leach-Bliley Act (GLB).[22]

The matter of the Privacy shield took place in the US, which directly came under direct pressure from the EU, and that led to the verdict in Schrem's Case,[23]where there was a high report of significant violations in the creation of the privacy shield.[24]

Some of the loopholes in the privacy shield as laid down by Max Shreams,[25]is kind of a lighter, up-to-date version, and the same came up in Max Schreams v. Data Protection Commissioner.[26]

[18] https://en-academic.com/dic.nsf/enwiki/170316

[19] Directive 95/46/EC on the protection of personal data https://en-academic.com/dic.nsf/enwiki/170316

[20] Ibid

[21] Roe v. Wade. 410 U.S. 113 (1973)

[22] Horrall, T. R., Pirn, R., & Markham, B. (2003). Instrumentation for measuring speech privacy in rooms. Journal of the Acoustical Society of America. https://doi.org/10.1121/1.4780900

[23] https://curia.europa.eu/juris/liste.jsf?num=C-362/14

[24] https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2016/cs2016_0076.

[25]The activist who took the case of transfer of his facebook data to US authorities, which resulted into invalidation of the European Commission's decision and indirectly led to the creation of the privacy shield.

[26] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62014CJ0362

The Judicial Redress Act, signed by the US in reaction to Edward Snowden's revelations, and the USA Freedom Act restricting the monitoring of intelligence are underlined in yellow highlight.

The privacy regime started with the EU, known for its very stringent and stiff laws, where the party who looks into the privacy shield has to look into the DPD of the EU, famously known as the Data Protection Directive[27].

One of the recent developments has been the California Privacy Rights Act. This strengthens the CCPA further by introducing the California Privacy Protection Agency and improving the rights available to consumers under the act, as pointed out in.[28] The recent moves are more state-level enhancements to privacy laws; this comes when there are perceived gaps because no federal framework exists.

Thus, the data protection structure followed in the United States relies significantly on a very decentralized model for data protection whereby sector-specific law and state-level statutes feature as primary models. Though industry-specific protection gives an industry-wise model of protection, it does come with its set of shortcomings: unharmonized national standards.

C. In UK

Notably, the data protection regime in the United Kingdom has evolved rapidly in the post-Brexit world, and the UK GDPR now facilitates continuity through available national adaptations. The proactive nature of the regulatory environment reflects an old tradition that maintains data protection as a country priority.

In the case of the UK, we find that the rule-making body was cautious and protective for such a case in hand; they were waiting and watching for all the actions and inactions happening in and around the UK.

[27] Svetlana Yakovleva and Kristina Irion, The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection, 2 Eur. Data Prot. L. Rev. 191 201

[28] California Privacy Protection Agency. "California Privacy Rights Act (CPRA) Details."

Later, the Government proposed that whoever has the authority to use and handle the data must be responsible and protect privacy adequately. Definition of forms of threat to privacy was defined in a white paper arising from five particular distinctive features which were from computer,[29] and they are: -

01. They have to maintain a high data security system and have to adhere to the protection of those data
02. They have to make data accessible from all outsource points with protection
03. They must easily allow secure data transfer with high security from one system to another.
04. They have to provide the option for combining data in all possible ways.

Further ahead, the government came up with a white paper on computer safeguards for Privacy, which will be ruled by a public sector undertaking, and in turn, the government established a Data protection committee under the chairmanship of Sri Norman Lindop, which was reported in 1978.

When the EU, that is, the European Union, is taken into consideration as the front-runners in matters of data protection, it is needless to say that they had the best laws that persisted in the times.[30]

The matters from study GDPR[31](General Data Protection Regulation)[32] is the new law in the year 2018 as it has just simplified data protection with the EU along with the rise of the technologies with the need of time that has also[33] included cloud computing, storage of Big data and even included the modern-day villain the AI into the all the parts of our day-to-day life.

[29]White Paper, 'Computers and Privacy' (Cmnd 6353, 1975)

[30] Peter Blume, The Public Sector and the Forthcoming EU Data Protection Regulation, 1 Eur. Data Prot. L. Rev. 32 2015, page-1, Rules relating to protection of data and personal data handled by public and private authorities are old and dates back to 1960s in EU,

[31]Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, 2016)

[32]http://usir.salford.ac.uk/id/eprint/60051/1/The%20General%20Data%20Protection%20Regulation%20%28GDPR%29%2C%20emerging%20technologies%202018.pdf

[33] Information Commissioner's Office, UK. "UK GDPR Compliance and Enforcement."

The UK GDPR is a version of the post-Brexit adaptation, maintaining core principles from the EU GDPR, but it still allows for some specific national modifications. The ICO remains the driving force in enforcing data protection regulations and in issuing guidance on compliance. The UK's ability to significantly and be actively involved in public education regarding data rights and responsibilities speaks for the high standard of data protection maintained in the UK. With an adaptation of the GDPR framework, the UK maintains high standards of data protection. The enforcement and public education of the ICO continue to strengthen the UK's commitment to the protection of personal data and compliance.

III. COMPARISON

In the Indian laws and the situation when we compare, we can clearly see the breach of the laws in India, whereas, on the other hand, we can see that in The UK there, they take an approach of waiting and watching to see the heinous crimes relating to the data breach and they establish the laws relating to the same and on the other hand they later establish the white paper to deal with the crimes relating to data breach and in the same time when US is taken into consideration we can see that they have the most of the laws in favor of the citizens where they combine one or more laws to take action to the data breach like FTCA and HIPPA.

More recently, India's approach has gained much momentum with the Digital Personal Data Protection Act, 2023 (DPDPA),[34] which is centered on a consent-based model that requires explicit consent for the processing of data.[35] This is in contrast to the GDPR of the EU, which provides multiple legal bases for data processing beyond consent, such as legitimate interests or contractual necessity. The stringent requirements for consent by India are an effort to empower the individual, although there are issues of enforcement and implementation.

The UK, which has so far adopted the cautious "wait and watch" approach, has transformed with the introduction of the UK General Data Protection Regulation (UK GDPR) post-Brexit.[36] Though the UK GDPR resembles the EU GDPR at every step, it does open the door to some

[34] Ministry of Electronics and Information Technology, Government of India. "Digital Personal Data Protection Act, 2023."DECODING DPDPA – India | Law Firm in Ahmedabad. https://amlegals.com/white-paper/decoding-dpdpa-india/

[35] Sharma, P. (2023). "The Consent Framework under the DPDPA." Journal of Data Privacy and Protection.

[36] UK Government. "UK General Data Protection Regulation (UK GDPR) Guidance."

domestic interpretations. The UK Data Protection Act 2018[37] supports the UK GDPR in a comprehensive system that addresses many modern data protection issues, from automated decision-making to data portability.

On the contrary, the United States does not have a whole-of-federal law on data protection, but sectoral laws are applied across different spheres of life, including the HIPAA and FTC Act. Other than these approaches, the federal state has even complemented its efforts with state-led approaches, the California Consumer Privacy Act being[38] among them, an act that bestowed on its consumers all rights for control over their information, including making opt-out and deleting data, among others.

Another significant aspect is that the US enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act,[39] which facilitates access agreements on data between the US and other countries, hence providing a clear alternative to the stringent cross-border transfer rules the EU has put in place with the GDPR.

Yet another divergence between India's and the US and UK's models is evident through the country's focus on data localization as contained in DPDPA. Under this model, critical personal data must be stored and processed in India. India thus shows strategic priorities to national security and sovereignty in handling data as much as it attracts public debate with implications for international business operations and global data flows.

In summary, the UK has refined its regulations more and more to meet the standard set by GDPR. At the same time, the US goes for pragmatic and sectoral policies with big-state-level innovation, and India continues striving to put together a solid legal framework, albeit heavily based on the concepts of consent and data localization. So, each country reflects different priorities legally, culturally, and economically regarding how this challenge of data protection should be faced.

[37] Data Protection Act 2018 Summary - DPA - Cookiebot™. https://www.cookiebot.com/en/data-protection-act-2018/
[38] California Legislature. "California Consumer Privacy Act (CCPA) Overview."
[39] United States Department of Justice. "Clarifying Lawful Overseas Use of Data (CLOUD) Act."

IV. TECHNOLOGICAL AND ETHICAL IMPLICATIONS AND FUTURE DIRECTIONS

Technology's rapid evolution has deeply affected the way data is collected, processed, and put to use. As such, while it has fully and fundamentally opened doors to terrific innovation and efficiency, the implications are as challenging as they are multifaceted in terms of ethical and legal aspects. The coming together of AI, Blockchain, and the IoT brings a new dimension to data governance, raising challenges for regulators across the globe. For India, the United States, and the United Kingdom, each of which has a different legal framework, these issues are best met by balancing technological development with the safeguarding of fundamental rights.

It thus highlights the trend of data security and the infringement of privacy through India's Digital Personal Data Protection Act 2023. A similar pattern in the United States is observed due to sector-specific data protection laws, while that of the United Kingdom shows a more relevant approach by bringing it in line with the General Data Protection Regulation approach. The following paper looks at these technological as well as ethical challenges concerning AI, Blockchain, and IoT in convergence with legal regimes.

A. Technological and Ethical Implications

i. Artificial Intelligence

Vast datasets AI depends on for learning are mostly filled with historical biases, particularly in discriminating people in hiring, law enforcement, and lending. Such non-transparent decision-making makes it difficult to have accountability, too, like when AI-powered surveillance tools are used by the public in a large scale during the COVID-19 outbreak concerning privacy and mass surveillance issues. Such problems demand solutions in India along with responsive legal frames that are non-discriminatory and transparent yet protect fundamental rights as provided for under Article 21 of the Constitution.[40]

It remains true that within its own domain of varied jurisdictions, the US implements acts to oversee sensitive information. Nonetheless, issues such as the case of Max Schrems v. Data Protection Commissioner[41] *emphasize a much stronger regulation and supervision of data flow across national borders. Within this framework, GDPR in the UK offers better accountability*

[40] 'India's Advance on AI Regulation' (Carnegie Endowment for International Peace, November 2024) https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation?lang=en&center=india

[41] C-362/14, ECLI:EU:C:2015:650

to AI implementation processes but leaves loopholes for various types of discrepancies during the implementation process. There are also questions of ethics relating to informed consent, algorithmic transparency, and the social impacts of automated decision-making systems.

ii. Blockchain and IoT

Blockchain is decentralized and immutable, which presents unique privacy challenges. Privacy laws like the European Union's right to be forgotten[42] contradict blockchain as it is made. For example, public ledger entries in blockchains do not alter or delete but create a scenario of non-compliance with current privacy laws because jurisdictions create problems, too, because decentralized means multiple countries might be involved. In contrast, each country would have its own form of law under which to operate.

IoT increases the scope of the data network by incorporating connected devices, producing massive amounts of sensitive data.[43] Cyber-attacks and data breaches similar to the COVID-19 data management in India revealed the vulnerability of IoT systems. These devices mostly lack advanced security features and are prone to exploitation. For instance, unsecured IoT devices become the entry points for hackers and expose the whole network. There is a need for legal frameworks around threats such as those above with evolving security by design and periodic compliance audits from manufacturers.

The framework of India's Digital Personal Data Protection Act 2023[44] can be seen for addressing data breaches. Still, compared to sector-specific laws within the United States and the compliance measures of GDPR in the UK, its enforcement mechanisms remain underdeveloped. For instance, sectorial-level cooperation exists in the United States for IoT security regulations. On the other hand, the UK encourages proactivity using white papers defining best practices related to cybersecurity. The Indian government must bridge such gaps by introducing strictly regulated policies that are written primarily for IoT systems.

[42] Finck, M. (2018). "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?" European Data Protection Law Review.
[43] Roman, R., Najera, P., & Lopez, J. (2011). "Securing the Internet of Things." Computer.
[44] The Digital Personal Data Protection Bill, 2023

iii. Ethical Concerns

Data commodification due to technological advancements treats people as a commodity whose data is traded without consent.[45] This raises issues of autonomy and privacy. For instance, the Cambridge Analytica scandal showed how voters' data was tampered with, epitomizing the dangers of unmonitored data use in an ethical sense.

Mass surveillance, empowered by advanced technologies, threatens civil liberties. For instance, when the Aarogya Setu app[46] was being implemented in India, privacy concerns arose, demanding that the oversight mechanism be very strong. In the United States, the Freedom Act and the UK, GDPR are attempts at finding a balance between security and privacy, although the challenges still lie in ensuring accountability and public trust.

The second problem is that data-driven profiling and predictive analytics may strengthen societal inequalities. Policymakers must engage with these ethical dilemmas in designing and implementing technological systems to incorporate the values of fairness and accountability.[47] Multi-stakeholder engagement in this matter involving civil society, academia, and the private sector would be necessary for the ethical application of technological systems.

B. Comparative Insight into Data Protection Frameworks

Comparing the data protection regimes of India, the United States, and the United Kingdom highlights that each differed markedly in the approach towards privacy. Although India's statute, primarily under the new Digital Personal Data Protection Act 2023,[48] has positioned stringent data protection measures for citizens, it also understands the necessity to bring it in concert with global standards. It hasn't reached its full potential due to delayed implementation

[45] Zuboff, S. (2019). "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power" PublicAffairs

[46] Ram, K. Janaki, Accessibility and Assistive Technology: A Case Study of Aarogya Setu Application (November 18, 2021). International Journal for Innovative Engineering and Management Research 2021, Available at SSRN: https://ssrn.com/abstract=3966011

[47] Sakshi Nanda, 'Ethical Considerations in Predictive Analytics: Ensuring Fairness and Accountability' (19 January 2024)

[48] Gail Crawford et al, 'India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison' (13 December 2023) GDPR, Legislative & Regulatory Developments

and weak enforcement of rules. One of the latest data breaches includes the breach in COVID-19 records, proving that proper oversight is needed.[49]

On the contrary, the system of law in the United States appears fragmented and deals with sectoral protections through enactments such as HIPAA or the Fair Credit Reporting Act.[50] These laws and statutes provide rigorous protection within various domains but hinder coordination in issues involving cross-border data governance both internationally and regionally. A corollary effect of Schrems II calls for data flow agreements from the transatlantic region to be harmonized.

The GDPR framework of the United Kingdom gives a single and integrated approach toward data protection by focusing on the rights of individuals and the accountability of the corporates.[51]Some provisions include "the right to be forgotten" and mandatory data breach notifications that will set the bar for transparency and consumer trust. The UK will have to reassess its data-sharing agreements with the EU and other countries after its transition from the EU.

C. Future Directions

i. Global Data Governance

International standards concerning data protection ought to be aligned.[52] Organizations, the United Nations as a case study, can act as catalysts in creating outlines regarding jurisdictional concerns and aligning data protection across borders from a harmonized global approach.[53] Standardization, aligned for international groups, helps the compliance function for multi-national corporations; inspiring consumer confidence still requires joint, collective focus on emerging innovations: quantum computers can break modern encryption levels currently.

[49] Anirudh Burman, 'Understanding India's New Data Protection Law' (3 October 2023)

[50] Gail Crawford et al, 'India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison' (13 December 2023) GDPR, Legislative & Regulatory Developments

[51] Ibid.

[52] National Institute of Standards and Technology, 'NIST Releases First 3 Finalized Post-Quantum Encryption Standards' (8 August 2024) https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[53]Ibid.

ii. Corporate Accountability

Data misuse can be prevented only if there are strict compliance measures in place. Regular audits, transparency reports, and stringent penalties for breaches should be implemented. For example, companies functioning in India[54] need to comply with both domestic law and international regulations to ensure sound data protection. Surprise inspections must be allowed for regulatory bodies to impose penalties as per the level of violation. Whistleblower protection mechanisms can also prompt employees to blow the whistle on unethical practices within organizations.[55]

iii. Public Awareness

Ensuring that people understand digital literacy would be the only way to ensure their privacy is protected.[56]This requires that curriculums in schools and community workshops address issues of data protection and online safety to close this gap. Knowledge of this gap can be the springboard that helps make an informed decision in protecting data.[57] Tools can be developed between the government and tech firms that make managing privacy settings an easy affair.

Digital literacy is also needed to campaign for the most vulnerable populations, including the aged and people living in rural settings away from conventional structures of learning. Mass media campaigns, online courses with engaging participation, and community-based sessions may help heighten public awareness.

In a nutshell, technology and ethics focus on flexible legal frameworks for data protection. Some of the issues in India, the US, and the UK are biased AI, blockchain, and IoT. Such issues necessitate collaboration toward setting global standards. Corporate accountability will be fostered, along with a public movement to raise public awareness, enabling society to be aware of all issues related to data protection in a digital world.

---

[54] 'Sarbanes–Oxley Act' (Wikipedia) https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

[55] Unveiling The Shadows: Types of Dark Web Threats - Candio. https://candio.co.uk/2023/11/23/unveiling-the-shadows-types-of-dark-web-threats/

[56] M Claire Buchan, Jasmin Bhawra, and Tarun Reddy Katapally, 'Navigating the Digital World: Development of an Evidence-Based Digital Literacy Program and Assessment Tool for Youth' (2024) Smart Learning Environments https://doi.org/10.1186/s40561-024-00293-x

[57] Ibid.

Technological innovation and privacy can definitely go hand-in-hand, though this will depend on concerted efforts to uphold both ethical standards and legal protections. The regulation of AI, Blockchain, and IoT will define what the balance of progress and preserving fundamental rights really means. In all this, policymakers, corporations, and individuals have something to do so that their respective technological innovations can benefit society while respecting the freedom of the individuals.

V. CONCLUSION AND RECOMMENDATION

Data breaches, data piracy, and data sharing have increased in the present world—even among government officials. Cases like 'Sprinklr' in Kerala bring to the forefront the involvement of the government in violating the fundamental rights under Article 21 of the Constitution. Involvement by the government in such scenarios is surfaced through inquiry. Fundamental rights have long back been declared as the basic structure of The Indian Constitution in *Keshavanada Bharathi v. State of Kerala*,[58] and it is also one of the fundamental aspects of the Constitution.

UK policymakers "wait and watch" data piracy, weighing its magnitude and social implications. The 'White paper' was created by the government to provide law and order along with minimum rights. US regulations are, however, vaster and more interdependent, which gives the warranty of data security and stops further crimes.

As we can see, in the case of the US, the laws were nearly stringent and were always to be read with other laws which co-existed in the matter. More significantly, cyber threats are ever-changing; hence, keeping the frameworks relating to data protection updated and at par is indispensable for all nations. To that extent, India is aiming to frame an all-round law structure for securing personal data coupled with a practice of holding processors accountable for misuse of it. It will be worthwhile in this respect when data protection officers and obligatory notification of breaches are featured in DPDPA.[59]

After Brexit, the UK has adopted its approach to the regulations so as not to leave out international requirements while maintaining some home comforts. For instance, the UK's

[58] AIR 1973 SC 1461

[59] Ministry of Electronics and Information Technology, Government of India. "Data Protection Officer Roles under the DPDPA."

Information Commissioner's Office has continued issuing guidelines and meeting penalties as a form of enforcing compliance; it also depicts the UK's seriousness on the matter.[60]
Even in the United States, despite not having a unified federal law, state-level laws like the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA) seem to reflect an inclination toward a stronger framework for data privacy. Such legislation looks forward to making its residents more empowered regarding personal data, with the companies becoming responsible users of personal data.[61]

The need for flexible legal frameworks also intensifies from the technological and ethical implications of emerging technologies in AI, Blockchain, and IoT.[62]Ethics of bias algorithms in AI and data commodification, mass surveillance, and surveillance capitalism highlight the imperativeness of global cooperation toward stringent data governance. Balancing technological innovation against individual privacy rights and ensuring accountability and public trust is necessary for these challenges to be addressed.

VI. SUGGESTIONS

The legislators must make hardcore efforts to understand the importance of the 'Data' and the violations and piracy matters that are becoming a global trend and have efforts to propose the best legislation to this effect so as to make sure there is enough protection that will be granted to their citizens as a matter of their right under the Article 21 of the Constitution of India which comes under the Part III of the Constitution.

Once the data breach happens, there should be laws that are internationally applicable as we have the lack of extra-territorial effect of the data because these days, all the crimes are committed online, and we can clearly see how the police are not having the jurisdiction and thus the laws making power or laws granting power to the police of the country to tie up with the INTERPOL and other various police agencies in an out of the world should be made.

There should be research made to comprehend the international impact of the protection that data is accorded and, hence, the protection of data with a more accurate effect.

---

[60] Information Commissioner's Office, UK. "Guidelines on Data Protection Compliance Post-Brexit."
[61] National Conference of State Legislatures. "Overview of State Data Privacy Laws."
[62] A Makanadar, 'Digital Surveillance Capitalism and Cities: Data, Democracy and Activism' (2024) 11 Humanities and Social Sciences Communications 1533 https://doi.org/10.1057/s41599-024-03941-2

Governments may, therefore seek to evolve international data protection alliances with the provision to cooperate across geographical boundaries in instances of cross-border data breach. The alliances shall ensure the facilitation of exchanging best practices, harmonizing laws, and responses to cyber-attacks in unison.

Public awareness initiatives on data privacy rights and good practice in digital practice should be used to empower individuals to protect themselves. Programs, both for the education of the consumer and for educating businesses, have to be provided to create a culture of protecting data.

Published by:

The Registrar
National Law Institute University Bhopal
(M.P.) 462044 INDIA