Automating Justice and Privacy: A Legal Critique of AI-Based Online Dispute Resolution in the view of Indian Data Protection Regimes

Authored by: Dr. Dharmendra Kumar Kumawat

Assistant Professor, Faculty of Law,

Guru Kashi University, Talwandi Sabo, Punjab, India

Co- Author-Prof. Deepak Kumar Chauhan

Professor, Department of Law, School of Legal Studies,

Central University of Punjab, Bathinda, Punjab, India

- **Abstract**

Since AI provides efficient, cost-effective, and user-friendly substitutes for conventional court processes, it is having a growing impact on the architecture and operation of Online Dispute Resolution (ODR) systems. However, there are serious issues with the use of AI in legal decision-making, especially with regard to accountability, algorithmic bias, and data protection. It is crucial to determine if the current legal framework is adequate to regulate the use of AI in legal services in light of the Digital Personal Data Protection Act of 2023, which India just approved. This article critically examines how AI-based ODR solutions conform with India's data protection legislation and constitutional requirements. The study offers a fair and moral framework that protects user rights, guarantees transparency, and maintains the integrity of justice delivery in the digital era, drawing on international regulatory frameworks like the EU's GDPR and the US sectoral model.

Keywords: Artificial Intelligence, ODR, Data Protection, Privacy Rights, DPDP Act 2023, Algorithmic Fairness, Legal Ethics, Indian Constitution, Digital Justice, AI Regulation

1. Introduction

The global health crisis induced by COVID-19 accelerated digital transformation across industries, and the legal sector was no exception. As litigation dockets grew increasingly congested, alternative pathways for dispute resolution became necessary. As an instrument for Alternative Dispute Resolution (ADR) processes, artificial intelligence (AI) began to show promise within this paradigm, offering scalable, practical, and easily accessible ways to handle a range of problems. The legal process is already beginning to benefit from artificial

intelligence (AI), which can help with decision-making and automate legal research and document analysis. The shift to technology-assisted adjudication has raised questions about the scope and feasibility of artificial intelligence's participation in conflict resolution. As digital justice gains popularity, especially in civil, consumer, and corporate disputes, integrating AI into Online Dispute Resolution (ODR) platforms is not just feasible but inevitable.

A critical analysis of the emergence of AI in dispute resolution is necessary. Significant ethical, legal, and procedural issues are brought up by such automation, even if AI can support human neutrals in arbitration or even act as an independent decision-making mechanism in simpler cases.AI-driven ADR systems promise faster, more affordable, and seemingly objective results. They could affect the complex human judgment needed to understand morality, justice, and the socio-legal context. Furthermore, as AI systems become increasingly adept at deriving conclusions from large legal databases and comprehending plain English, concerns regarding data privacy, algorithmic bias, and accountability grow. This paper explores whether the institutional adoption of AI-based ADR in India is aligned with the country's constitutional and legal commitments—especially under the recently enacted Digital Personal Data Protection Act, 2023—while drawing on comparative insights from global jurisdictions to propose a balanced, rights-centric framework for responsible AI integration in the justice system.

1.1. Review of Literature

The research on Online Dispute Resolution (ODR) powered by AI emphasizes how important it is becoming to improve access to justice through technology. The evolution of ODR from conventional ADR techniques to tech-driven platforms with AI tools for arbitration and negotiation is described by Yash Pathak (2025).While benefits such as cost-effectiveness and cross-border accessibility are emphasized, concerns regarding privacy, fragmented regulations, and ethical oversight persist. This work also looks at India's advancements in ODR through policy backing, legal recognition, and programs like SAMA and CORD, emphasizing strong infrastructure, regulations, and trust-building strategies for successful execution. Expanding upon this, Marco Giacalone (2025) investigates further how AI enhances productivity and user accessibility while warning about potential hazards such algorithmic bias, opaque decision-making, and inadequate regulatory protections.The study emphasizes the significance of incorporating human judgment, bolstering data protection measures, and incorporating ethical

principles—especially in India's changing legal context—in order to preserve fairness and procedural integrity in technology-assisted dispute resolution.

Building further, Pallavi Bhardwaj and Sanighdha (2025) delve into how artificial intelligence is reshaping the mechanisms of alternative dispute resolution in contemporary legal frameworks. The authors examine the growing use of AI in processes such as predictive outcome analysis, automated dispute settlements, and digitized platforms like e-Lok Adalats. Along with the associated worries about transparency, ethical oversight, and the absence of emotional intelligence in machine-driven judgments, this study highlights the potential for increased accessibility and efficiency. In order to guarantee that technological advancement does not jeopardize justice or equity, the study promotes a deliberate approach to integrating AI into India's ADR system, emphasizing the significance of combining human judgment, context sensitivity, and constitutional protections.

Further, Md Junaid's (2024) work supports this study and provides a detailed examination of how AI is changing online arbitration inside the Indian legal system. The author highlights how artificial intelligence (AI) increases the effectiveness of case administration, facilitates decision-making using predictive tools, and increases accessibility to arbitration, especially in rural regions. The study examines how platforms such as Presolv360 and ODR methods are simplifying arbitration processes and highlights India's developing digital legal infrastructure. It also recognizes enduring issues, including insufficient digital infrastructure, weaknesses in data privacy, and opposition from conventional legal actors. In order to guarantee equitable and transparent dispute resolution procedures, the paper promotes ethical standards, public-private partnerships, and hybrid models that combine human judgment with AI capabilities, taking inspiration from countries such as Singapore, the UK, and the US. The study strengthens the argument that India must balance technological advancement with legal accountability to build a resilient and inclusive AI-driven arbitration framework.

The study of Nadia Ahmad (2025) offers provides a thorough analysis of how AI may be integrated into ODR platforms. It describes how AI-driven technologies, such as chatbot-assisted mediation and automated document review, improve procedural speed, save costs, and place the needs of users at the center of conflict resolution. The study also highlights issues with interpretative justice's shortcomings, the over-reliance on automated reasoning, and the

exclusion of litigants with low levels of computer literacy. It highlights the need for inclusive design and algorithmic transparency and calls for the incorporation of AI technology within a legal framework that prioritizes accountability, consent, and equity. The authors suggest a hybrid ODR paradigm that preserves the fundamentals of natural justice in digital contexts by fusing human judgment with computer efficiency.

The ethical issues raised by AI-driven technologies in managing personal data are examined in the paper by Jose Ramon Saura et al. (2024), especially in light of consumer profiling and targeted decision-making.Despite the study's focus on digital marketing, its conclusions are extremely applicable to AI-based Online Dispute Resolution (ODR) since both fields entail automated systems handling private user data. The analysis highlights a growing privacy paradox where users trade convenience for data management by criticizing the unbalanced relationship between personalization and user autonomy. It argues for stricter regulatory oversight, ethical AI design, and transparency in data handling—principles equally essential for ensuring fairness and accountability in AI-integrated ODR systems.

A thorough analysis of how AI technologies are changing conventional dispute-resolution procedures is provided by Hibah Alessa (2022).It demonstrates how AI may be used practically to streamline procedures like document analysis, case screening, and prediction-based suggestions. Because of the lack of transparency, potential bias, and less human involvement in decision-making, the study warns against relying too heavily on automated systems. It comes to the conclusion that, even if AI can be a useful aid in ODR, its application needs to be carefully controlled, with a focus on ethical alignment, human oversight, and due process to protect the administration of justice.

While existing literature comprehensively explores the efficiency, accessibility, and ethical implications of AI in Online Dispute Resolution, a critical gap remains in examining the intersection between AI-based ODR systems and data protection laws within the Indian legal framework. Most studies emphasize procedural automation and general ethical concerns, but few provide a focused analysis of how emerging legal instruments such as the Digital Personal Data Protection Act, 2023, interact with AI-driven ODR platforms. There is limited scholarly engagement with questions of user consent, algorithmic accountability, and compliance with constitutional principles such as the right to privacy. By critically evaluating whether the current data protection laws in India provide sufficient protections for the responsible

application of AI in ODR and by putting forth a rights-based regulatory framework based on openness, due process, and human dignity, this study aims to close that gap.

1.2. Statement of the Research Problem

There are advantages and disadvantages to India's increasing usage of AI in online dispute resolution procedures. These techniques speed up dispute resolution and improve accessibility, but they also bring up fresh ethical and legal issues. Notably, the lack of explicit regulatory standards to govern automated decision-making in ODR creates uncertainty about privacy protection, transparency, and accountability. The central problem addressed in this research is whether the existing Indian legal framework—including the Digital Personal Data Protection Act, 2023—is sufficient to govern the ethical deployment of AI in dispute resolution, and if not, how it might be restructured to fill this critical regulatory void.

1.3. Objectives of the Study

1. To analyse the extent to which AI-based ODR systems conform to India’s data protection and constitutional legal norms.

2. To develop a rights-oriented regulatory framework for ethical and accountable use of AI in ODR mechanisms.

1.4 Research Questions

• Do AI-powered ODR platforms comply with the constitutional and data protection standards in India?

• What are the inherent legal and ethical concerns related to automation in dispute resolution?

• What framework can ensure both technological innovation and fundamental rights in the context of AI-assisted ODR?

1.5. Hypothesis

In the absence of tailored legal provisions and oversight mechanisms, AI-based ODR systems in India risk undermining constitutional rights such as privacy, equality, and access to justice.

1.6. Research Methodology

This research used doctrinal legal analysis, focusing on relevant statutes, constitutional provisions, and judicial pronouncements related to AI, privacy, and dispute resolution in India. The study integrates a comparative methodology by reviewing regulatory approaches from international jurisdictions, particularly the EU and the United States, to identify adaptable frameworks for India. A critical and comprehensive overview of the issues is provided by secondary sources, which include scholarly literature, existing policies, and legal documents. The study concludes with policy suggestions meant to guarantee that the incorporation of AI into ODR is consistent with democratic principles and the rule of law.

2. Legal and Regulatory Framework in India

The enactment of the Digital Personal Data Protection Act of 2023 has significantly refined India's approach to safeguarding privacy and data online. This law broadens its purview to encompass data handled both domestically and abroad if it is linked to goods and services intended for Indian nationals. The Act introduces key principles around consent, purpose limitation, and obligations for data fiduciaries, including special provisions for children's data and penalties for non-compliance. Crucially, it takes the place of previous safeguards provided by the Information Technology Act of 2000 and the SPDI Rules, signifying a shift from disjointed governance to a single, rights-based data protection framework. India's intention to harmonize digital administration with constitutional values—specifically, the right to privacy—is emphasized by this framework.

In addition to data protection, the broader digital governance architecture is being shaped by institutions like MeitY, CERT-In, and TRAI. MeitY has expanded its digital vision through the extension of the Digital India Programme until 2026, emphasizing inclusive access to e-governance and AI-enabled tools like Bhashini. CERT-In has introduced cybersecurity guidelines for government agencies, mandating roles such as Chief Information Security Officers and emphasizing regular audits and threat monitoring. Meanwhile, TRAI has proposed the establishment of a dedicated authority—Artificial Intelligence and Data Authority of India (AIDAI)—to oversee responsible AI use. This multi-stakeholder regulatory vision reflects India's recognition of the growing complexities of algorithmic governance and the need for both technical and ethical supervision.

The changing judicial-tech nexus in India is also indicated by parallel developments. By creating a contemporary adjudicatory procedure specifically designed for online civil and

criminal disputes, the proposed Digital India Act seeks to replace the antiquated IT Act, 2000. The Act is expected to incorporate robust accountability structures, uphold constitutional protections under Articles 14, 19, and 21, and encourage ethical AI practices. Furthermore, initiatives like Aadhaar authentication using AI-driven liveness checks, the inclusion of Virtual Digital Assets under the Prevention of Money Laundering Act, and draft cybersecurity guidelines for Payment System Operators collectively illustrate a forward-looking digital legal ecosystem.These efforts signal a growing acknowledgement that technological innovation must be accompanied by strong legal frameworks to preserve individual rights and promote trust in digital systems.

3. Data Protection and Privacy Concerns

In addition to speeding up India's digital growth, the Digital India initiative and the widespread use of AI technologies in fields like payments, governance, and judicial administration have raised urgent concerns over algorithmic processing, authorization, and personal data ownership. The Digital Personal Data Protection Act, 2023 (DPDP Act) creates rules for consent, permitted processing, and data management responsibility in order to address these problems. However, there are still many ambiguous and interpretable phrases, particularly in relation to AI's use of personal data and automated decision-making. For example, even while the Act recognizes automated technology fall under its scope, it does not directly address artificial intelligence, which allows for interpretational ambiguity. Unrestricted AI model training is made possible by excluding publicly available data from protection, which may be against privacy laws. In addition, by hiding data collection, processing, and third-party sharing—particularly on state-run platforms like UMANG—the Act's vague consent procedures defeat its goal of ensuring informed user control.

Equally concerning are the systemic risks associated with surveillance, profiling, and lack of algorithmic transparency. Section 7 of the DPDP Act permits non-consensual data processing in the “public interest,” but without a clear definition, this clause risks legitimizing mass surveillance under vague justifications.[ ] Previous incidents, including the use of facial recognition technology during protests, underscore the potential for violations of Article 21 rights and state overreach. Similarly, issues with welfare disbursements connected to Aadhaar raise concerns under Article 14 since they demonstrate how computational errors can disproportionately affect vulnerable people. Despite being crucial historically, the Information

Technology Act of 2000 no longer sufficiently tackles these new concerns; its rules on data breaches, intermediary responsibility, and surveillance are insensitive to problems caused by artificial intelligence. Legal protections need to change as synthetic content and predictive analytics become more prevalent. The new Digital India Act is expected to bridge these gaps and align technological innovation with ethical commitments and constitutional values by establishing more detailed criteria for AI responsibility, content control, and user protection.

4. Constitutional and Jurisprudential Analysis

The 2017 ruling in Justice K.S. Puttaswamy v. Union of India significantly changed India's constitutional landscape by preserving the right to privacy as a fundamental right protected by Part III of the Constitution.[ ] Delivered by a nine-judge bench of the Supreme Court, the decision overruled earlier judgments in M.P. Sharma and Kharak Singh, establishing that privacy is intrinsic to Articles 14, 19, and 21.[ ][ ] Although six separate opinions were delivered, all judges unanimously agreed that privacy is a natural, inalienable right encompassing autonomy, dignity, bodily integrity, and informational control. With a strong emphasis on both State and non-state intrusions, several privacy-related topics were covered d, including rest, sanctuary, and prison-station-making. The ruling also recognized the necessity for strong statutory protection in light of the growing concerns associated with the digital age, including mass spying, data mining, and profiling. Importantly, it recognized privacy not only as a negative right (freedom from intrusion) but also as a positive obligation on the State to ensure protective legal frameworks.

The Court further provided doctrinal clarity by articulating judicial standards for assessing privacy violations. A consensus emerged around the application of a structured proportionality test—comprising legality, legitimate aim, proportionality, and procedural safeguards—to evaluate State interference. Justice Chandrachud's framework emphasized that any restriction must be backed by law, serve a legitimate purpose, and maintain a rational nexus between means and objectives. Justice Kaul extended this by incorporating the European "least restrictive means" test and the requirement for procedural checks. Article 21 mandates that any violation of privacy must always pass the fairness, proportionality, and necessity test, even when privacy is not regarded as absolute. Since then, the ruling has become the cornerstone of India's constitutional privacy-related legislative changes, which are especially pertinent in light

of data security, digital monitoring, and developing artificial intelligence. Puttaswamy continues to be a fundamental point of reference for striking a balance between technology advancement and individual rights and freedoms as courts and legislators face new difficulties brought on by digital technologies.

4.1. Challenges of Ensuring Fairness and Accountability in AI

Significant legal issues pertaining to algorithmic accountability and fairness have arisen in India as a result of the quick adoption of AI in industries including healthcare, banking, government, and transportation. Traditional legal systems, rooted in human decision-making, lack the conceptual tools to assign responsibility when autonomous AI systems cause harm—such as through discriminatory credit scoring or flawed medical diagnoses. Liability for AI-driven errors is not yet well defined by Indian jurisprudence, including tort and contract law, which raises questions about who is responsible—developers, users, or the AI systems themselves. The opacity of AI algorithms further complicates this, making it difficult to trace or audit decisions, especially when proprietary algorithms are used in public decision-making. Cases like Rajendra Singh v. State of Rajasthan and Indian Medical Association v. Union of India demonstrate judicial concern over unregulated AI usage in sensitive areas yet underscore the absence of legislative clarity and a framework for establishing legal culpability in AI outcomes.

Additionally, ensuring fairness in AI systems is hampered by the inherent biases embedded in training datasets. When societal inequities around caste, gender, or religion are reflected in the data, AI systems risk replicating and institutionalizing discrimination. Predictive analytics and face recognition are two tools that are being utilized more and more in public administration, but their propensity to mistakenly identify members of underrepresented groups has sparked concerns. These arrangements jeopardize basic rights guaranteed by Articles 14, 15, and 21 of the Indian Constitution in the absence of governmental monitoring. Although the Supreme Court's judgment in K.S. Puttaswamy v. Union of India laid a constitutional foundation for protecting privacy, it did not resolve AI-specific questions about bias and transparency. Therefore, there is an urgent need for a specific legislative framework that includes ethical standards, requires algorithmic audits, and establishes accountability systems to guarantee AI functions in a way that respects human dignity and constitutional values.

5. Comparative Jurisdictional Insights

With the General Data Protection Regulation (GDPR) and the planned AI Act, the European Union provides a strong legal framework for regulating AI and data protection.The GDPR emphasizes transparency, user consent, and the right to explanation in automated decision-making, thus setting a high standard for data privacy. The upcoming AI Act categorizes AI systems according to danger tiers, outlawing high-risk uses like social rating and tightly regulating industries like vital infrastructure and biometric monitoring. When combined, these tools offer a thorough framework for defending individual liberties and promoting creativity in the application of AI.

The US, on the other hand, takes a sector-specific approach to data and AI governance, emphasizing industry-by-industry supervision over a single regulatory framework. For example, the Health Insurance Portability and Accountability Act (HIPAA) governs health data, while the Fair Credit Reporting Act (FCRA) covers financial services. This strategy encourages adaptability and quick adoption of technology, but it frequently results in uneven safeguards and enforcement gaps, especially when it comes to cross-sectoral AI applications. The necessity for broad ethical and legal boundaries is becoming more widely recognized, as seen by recent initiatives like the Blueprint for an AI Bill of Rights and executive directives on trustworthy AI.

These comparative frameworks provide important insights for India. The U.S. approach emphasizes the necessity for flexibility in innovation-driven industries, whereas the EU's rights-based, risk-tiered regulation emphasizes the need of proactive legislation based on constitutional principles. By creating a cohesive yet flexible regulatory framework that tackles sector-specific issues, encourages accountability, and guarantees algorithmic transparency, India must find a balance between these strategies. Incorporating global best practices into India's evolving regulatory landscape—especially in light of the DPDP Act, 2023—can help build public trust and align AI governance with democratic principles.

6. Towards Responsible AI ODR: Policy Recommendations

Maintaining justice and trust as India negotiates the use of AI in Online Dispute Resolution (ODR) requires that algorithmic decision-making be transparent and explicable. Early attempts to improve legal services through AI integration are shown in initiatives like SUVAS and AI chatbots. Algorithmic transparency, which allows stakeholders to comprehend how AI systems arrive at conclusions, is necessary for effective deployment, particularly when those findings

have an impact on legal decisions. The paper emphasises continuous monitoring and calibration of AI tools to mitigate bias and promote equitable decisions. Such transparency not only fosters trust among users but also aligns with constitutional guarantees of due process and fairness.

A further crucial aspect of integrating AI in dispute resolution is putting privacy-by-design principles into practice. With ODR platforms handling sensitive personal and legal data, robust data protection measures must be embedded at every stage of the system's architecture. Challenges related to data privacy, as highlighted by NITI Aayog and in global AI ethics discourse, necessitate the enforcement of strong safeguards that respect individual autonomy and the right to be forgotten. India's regulatory push through the DPDP Act, 2023, must be extended to AI-ODR mechanisms to ensure compliance, particularly in areas involving biometric data, profiling, or predictive analytics used in adjudication or negotiation.

Lastly, maintaining legal responsibility and public trust in AI-powered ODR systems requires human oversight and easily accessible grievance redress procedures. The paper advocates for human-in-the-loop models where human experts review or intervene in AI-generated outcomes, especially in complex or high-stakes disputes. In order for users to contest, appeal, or review automated judgments, clear grievance resolution channels must be established. Therefore, policy frameworks should require a hybrid model that combines human judgment with AI's efficiency to guarantee that justice is still participative, reviewable, and consistent with constitutional principles.

7. Conclusion

By improving efficiency, accessibility, and cost-effectiveness, the incorporation of artificial intelligence into Online Dispute Resolution (ODR) systems presents a once-in-a-lifetime chance to revolutionize the way justice is delivered. But basic rights, especially the rights to privacy, procedural justice, and individual liberty, must not be sacrificed for the sake of innovation. The legal and ethical challenges posed by AI—ranging from opaque algorithms and data misuse to bias and lack of accountability—necessitate a careful recalibration of priorities. Any violation of privacy or liberty must pass stringent legality, need, and proportionality criteria, according to India's constitutional framework, particularly after Putttaswamy. Therefore, achieving a balance between technological advancement and rights protection is not only desirable but essential for ensuring that justice remains human-centred in the age of automation.

To effectively develop AI-based Online Dispute Resolution (ODR) systems in India, we must establish a rights-based regulatory framework grounded in constitutional values, data protection standards, and international best practices. This necessitates implementing robust human oversight procedures, ensuring algorithmic openness, using privacy-by-design tactics, and providing effective routes for grievance resolution.

Although the Digital Personal Data Protection Act of 2023 offers a crucial legislative framework, it must be complemented by particular rules pertaining to legal technology. The need for flexible, responsible, and inclusive regulatory approaches is underscored by the lessons gained from the United States' sector-specific models and the European Union's General Data Protection Regulation (GDPR) and AI Act. By creating a coordinated and participatory framework, India can leverage the transformative potential of AI in dispute resolution while also protecting the dignity and rights of its citizens.

8.References

1. Alessa, H. (2022). The Role of Artificial Intelligence in Online Dispute Resolution: a Brief and Critical Overview. Information & Communications Technology Law, 31(3), 1–24. Taylor & Francis. https://doi.org/10.1080/13600834.2022.2088060
2. Acero, F. (2025). The Use of Artificial Intelligence in Arbitration: Friends with Benefits. Deleted Journal, 74. Vniversitas Jurídica. https://doi.org/10.11144/javeriana.vj74.uaia
3. Anexusadmin. (2025, March 24). AI Dispute Resolution | Faster, Fairer & Cost-Effective. NexLaw. https://www.nexlaw.ai/ai-dispute-resolution/
4. Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial Intelligence in Information Systems research: a Systematic Literature Review and Research Agenda. International Journal of Information Management, 60(102383). Sciencedirect. https://doi.org/10.1016/j.ijinfomgt.2021.102383
5. Pathak, Y. (2025). Pioneering Innovations in Digital Jurisprudence: Evaluating ODR Systems and AI In Shaping the Future of Conflict Resolution. SSRN Electronic Journal, 35. SSRN. https://doi.org/10.2139/ssrn.5110555
6. Giacalone, M. (2025). AI and the Future of Private Dispute Resolution Mechanisms. SSRN Electronic Journal, 16. SSRN. https://doi.org/10.2139/ssrn.5083207

7. 6.Bhardwaj, P. (2025). Redefining Dispute Resolution: The Intersection of Alternative Dispute Resolution and Artificial Intelligence in Law. International Journal of Law Management and Humanities, 8(2), 87–99. https://doij.org/10.10000/IJLMH.119085
8. Junaid, Dr. M. (2024). Justice Reimagined: The Role of Artificial Intelligence in India's Online Arbitration. International Journal for Multidisciplinary Research, 6(6), 1–9.
9. Ahmad, N. (2025). Smart Resolutions: Exploring the Role of Artificial Intelligence in Alternative Dispute Resolution. Cleveland State Law Review, 73. https://engagedscholarship.csuohio.edu/clevstlrev/vol73/iss2/6/
10. 8.Saura, J. R., Škare, V., & Dosen, D. O. (2024). Is AI-based Digital Marketing ethical? Assessing a New Data Privacy Paradox. Journal of Innovation & Knowledge, 9(4), 100597. ScienceDirect. https://doi.org/10.1016/j.jik.2024.100597
11. 9.Alessa, H. (2022). The Role of Artificial Intelligence in Online Dispute Resolution: a Brief and Critical Overview. Information & Communications Technology Law, 31(3), 1–24. Taylor & Francis. https://doi.org/10.1080/13600834.2022.2088060
12. 10.Saha, S., & Mukhopadhyay, S. (2024). A New Age of Data Privacy Laws in India: Review of Digital Personal Data Protection Act, 2023. International Journal of Law and Social Sciences, 10(1), 84–95. https://doi.org/10.60143/ijls.v10.i1.2024.114
13. 11. Desai, N. (2023, August 7). Nishith Desai Associates India's Digital Personal Data Protection Act, 2023: History in the Making. Www.nishithdesai.com. https://www.nishithdesai.com/NewsDetails/10703
14. 12.Dharmaraj, S. (2024, September 27). India's Commitment to Data Protection and Digital Governance – OpenGov Asia. Opengovasia.com. https://opengovasia.com/2024/09/27/indias-commitment-to-data-protection-and-digital-governance/
15. 13. Singh, K. (2025, May 16). Does Article 21 include right to digital access? | Explained. The Hindu. https://www.thehindu.com/news/national/does-article-21-include-right-to-digital-access-explained/article69580767.ece

16. 14. Burman, A. (2023, October 3). Understanding India's New Data Protection Law. Carnegieendowment.org. https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en
17. 15. Sombatpoonsiri , J., & Mahapatra, S. (2024). Regulation or Repression? Government Influence on Political Content Moderation in India and Thailand. Carnegieendowment.org. https://carnegieendowment.org/research/2024/07/india-thailand-social-media-moderation?lang=en
18. 16.Shiv. (2022, August 22). What were the Major Loopholes in the Data Protection Bill that led to its Withdrawal. Globalpolicyinsights.org. https://globalpolicyinsights.org/what-were-the-major-loopholes-in-the-data-protection-bill-that-led-to-its-withdrawal.php
19. 17.Justice K.S. Puttaswamy (Retd) and Anr. v. Union of India and Ors., AIR 2017 SUPREME COURT 4161.
20. 18. M. P. Sharma and Others v. Satish Chandra, AIR 1954 SUPREME COURT 300.
21. 19.Kharak Singh v. The State of U. P. & Others, 1963 AIR 1295.
22. 20.Jure Globocnik. (2024, October 16). GDPR and AI Act: similarities and differences | activeMind.legal. ActiveMind.legal. https://www.activemind.legal/guides/gdpr-ai-act/
23. 21.Edemekong, P. F., Haydel, M. J., & Annamaraju, P. (2024). Health Insurance Portability and Accountability Act (HIPAA). National Library of Medicine. https://www.ncbi.nlm.nih.gov/books/NBK500019