JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DATA GOVERNANCE IN THE AGE OF EMERGING TECHNOLOGIES: MULTIJURISDICTIONAL INQUIRY INTO PRIVACY AND ETHICAL IMPERATIVES FOR AI, IOT, & BLOCKCHAIN

Shreyaa D R, (10 BBALLB, 20113182), School of Law, Christ Deemed to be University, Lavasa, Pune, India
Dr. Chetan Dixit, (Assistant Professor), School of Law, Christ Deemed to be University, Lavasa, Pune

ABSTRACT

The advent of emerging technologies in the age of Artificial Intelligence (AI), Internet of Things (IoT), Blockchain has brought a level of unprecedented complexities in data governance, especially, with regards to data privacy, security and cross border regulatory issues. This paper examines the confluence by which these technologies meet transforming regulations, as well as the ramifications that result from data operations in decentralized and hyperconnected settings. It looks into the ways AI's data-dependent algorithms, IoT's real-time monitoring abilities, blockchain's eternal registries pose new necessities for adaptable systems of governing, and privacy sustaining technologies. The study provides a comparative analysis of international regulatory responses, such as European Union's General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL), and India's Digital Personal Data Protection Act (DPDPA), 2023 to show how different jurisdictions find the balance between innovation and privacy protection. In addition, the paper also disusses the roles played by such technologies such as federated learning, homomorphic encryption, and zero knowledge proofs in boosting data privacy. The paper concludes that there is a need for a unified response to the problem of data governance, which involves ethical AI principles, cross-border cooperation and technological safeguards, in order to guarantee responsible innovation and respect of individual rights in the digital world.

KEYWORDS

Data Governance; Artificial Intelligence (AI); Internet of Things (IoT); Blockchain Technology; Data Privacy; GDPR; PIPL; DPDP Act; Zero-Knowledge Proofs; Differential Privacy; Ethical AI; Unified Digital Regulation; Cross-Border Data Flow; Cybersecurity; Emerging Technologies

1. INTRODUCTION

The developing technologies including Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain have created complex issues for data protection which also present novel perspectives. The developing technologies make governments together with regulatory agencies globally confront decisions between supporting innovation and protecting privacy and security throughout the world. This paper analyzes how data governance interacts with new technologies as it considers both data privacy issues alongside regulatory variables as well as privacy-protected technologies and governing structure approaches.

Organizations use data as their most essential resource in present day digital operations and strategic planning and innovative development. Organizations use the term "data governance" to describe their system which defines the management and utilization of data alongside its sharing and protection processes. Multiple practices and standards and policies unite under the concept to protect data availability while ensuring data

security and integrity alongside usability. The increasing importance of robust data governance systems continues to intensify due to recent developments in AI and IoT and Blockchain which alter data generation and processing behaviors. The revolutionary capabilities of these technologies lead to unrelated data complexities and dangerous security risks for privacy data and regulatory compliance with ethical boundaries.

2. DATA PRIVACY CONCERNS IN AI, IOT, AND BLOCKCHAIN

The large-scale operation of emerging technologies generates substantial privacy-related problems and security issues that affect data management control. The problems from unstandardized global data protection regulations become worse because businesses need to solve many different sets of requirements across various legal systems for compliance purposes.[1]

Data governance is the strategic and operational scaffold used to describe the means of handling, safeguarding and leveraging data during the lifecycle. Effective data governance is something that is not only a requisite for compliance with regulation but an aspect necessary to sustain public trust and drive responsible innovation in today's digitized world. Emerging technologies change the landscape of data governance and form unstructured, distributed, and mysterious ecologies. AI algorithms, data-hungry and used for training/prediction purposes, IoT devices give live data-streams, while blockchain ledgers provide immutable transaction records–and they all curiously stretch the current legal/ethical frameworks.

2.1 ARTIFICIAL INTELLIGENCE (AI)

AI systems need extensive datasets to undergo training before they can make operational decisions. Multiple privacy-invading problems emerge when using algorithmic systems together with automated processes and facial recognition systems. Modern legal entities and healthcare institutions as well as financial service providers face criticism because their AI programs invade privacy rights of consumers. The regulatory bodies in the EU and U.S. focused their attention on ***Clearview AI*** *because of its unauthorized collection of biometric data.* AI functions more effectively to discover intimate information from basic data points thus intensifying privacy security issues.[2] Health-related applications powered by AI generate predictions about medical conditions using user behavior data which raises novel ethical problems about how users consent to these practices and conditions regarding data administration.[3] Modern deepfake technology powered by artificial intelligence creates identification risks and spread of false information which intensifies demand for strict regulatory control.[4]

AI applications requires companies to comply with multiple regulatory frameworks that include the GDPR of the European Union the PIPL and the evolving national AI strategies throughout different countries. The inconsistent definitions about consent along with data minimization rules and explanations rights across frameworks makes organizations need adaptable data governance solutions. AI governance depends on the practice of risk management. The widespread high-risk use of AI in healthcare and finance and criminal justice demands organizations to conduct thorough assessments followed by risk mitigation measures which emphasize transparency and security in addition to algorithmic accountability.

2.2 INTERNET OF THINGS (IOT)

IoT devices collect and transmit continuous streams of data, often without explicit user consent. Smart home devices, wearable health monitors, and connected cars generate sensitive personal data, making them vulnerable to cyberattacks and unauthorized access. ***The Ring doorbell privacy case***[5] highlighted risks associated with data breaches in IoT systems, emphasizing the need for stronger security measures.

The Internet of Things (IoT) serves as a major disruptive technology that makes data governance more difficult to navigate. Through IoT networks computers connect billions of physical devices which include

[1] Joshi, Navmi. (2024). Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence. International Journal of Law and Policy 2. 55-77. 10.59022/ijlp.171.
[2] ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292 DePaul University, *Journal of Art, Technology, and Intellectual Property*, DEP. UNIV. (2025), https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1651&context=jatip.
[3] Zag ElSayed et al., *Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions*, ARXIV (Jan. 20, 2025), https://arxiv.org/abs/2501.11250.
[4] Lawfare, *Human Subjects Protection in the Era of Deepfakes*, LAWFARE (Nov. 2, 2023), https://www.lawfaremedia.org/article/human-subjects-protection-in-the-era-of-deepfakes.
[5] Cloud Security Alliance, *Amazon Ring: A Case of Data Security and Privacy*, CSA (Mar. 26, 2022), https://cloudsecurityalliance.org/blog/2022/03/26/amazon-ring-a-case-of-data-security-and-privacy.

both consumer electronics like home thermostats and wearable fitness trackers and industrial instruments such as sensors along with autonomous vehicles that constantly transmit data. This data exists in a vast volume with multiple formats that show complex connection dependencies.[6] New data governance concepts are necessary to suit IoT environments because they possess distinct features. Mounting IoT-generated data must be analyzed and responded to speedily because devices produce real-time data collections. The data exists with two major issues: (1) it has strong local character and (2) contains sensitive content like health metrics and location information which requires advanced privacy measures and encryption standards.

A significant challenge with IoT security is the lack of uniform security standards, leading to inconsistent protection across different device manufacturers. In 2022, vulnerabilities in medical IoT devices were exploited by cybercriminals, compromising patient data and healthcare systems. This incident underscored the necessity of stricter cybersecurity protocols and real-time monitoring for IoT infrastructure.[7]

2.3 BLOCKCHAIN TECHNOLOGY

Data protection stands as a major challenge because blockchain operates in a decentralized system which maintains unalterable records. The enhanced security and transparency of blockchain platforms create an issue against GDPR privacy regulations which ensure users can be forgotten. People have privacy-related worries about blockchain-powered financial services and digital identity authentication mechanisms because they maintain permanent records and share identifying information openly. Privacy discussions about blockchain systems have gained focus in decentralized finance platforms because these platforms make transaction histories viewable on global public records.[8] **Blank-Knowledge Proofs (ZKPs)** function as promising privacy upgrades for blockchain systems that maintain security protections.

The field of conventional governance discussions fails to include detailed discussions about blockchain technology which brings both complications and new possibilities to modern governance systems. A decentralized immutable ledger system which blockchain delivers enables new ways for ensuring transparent and tamper-proof data sets.[9] Transactions within blockchain systems receive both timestamp confirmation and cryptographic protection thus creating a secure chronological record that helps auditors and regulators with compliance needs. Blockchains prove best suitable in scenarios demanding stringent trust and complete data traceability because of its superior data validation features—such as supply chains and identity verification and smart contracts. The dispersed operation of blockchain technology introduces obstacles when managing data control systems. The control power of data management rests with multiple distributed nodes instead of a centralized database authority. A fundamental question emerges regarding who owns the data along with the need for responsibility and the right to have information removed which particularly matters when enforcing GDPR data protection statutes. Blockchain data persistence conflicts with privacy laws because such laws enable people to remove or change their personal information. Developing governance structures for blockchain systems demands consensus about how to match blockchain properties with current laws and moral frameworks.

The joint operations of IoT with AI create expanded governance matters. Real-time analytics along with predictive maintenance capabilities and adaptive systems result from using AI algorithms to analyze IoT data. Combined IoT and AI operations create data tracing challenges which make it difficult to follow information sources or guarantee responsibility tracking. A traffic management system with AI-enabled IoT sensor technologies needs to confirm the safety of sensor data in addition to ensuring fair and lawful decisions from its decision-making processes. The data governance system needs to operate between sensors and algorithms to build an integrated framework ensuring end-to-end quality evaluations with auditing capabilities and ethical management of data.

3. REGULATORY APPROACHES: GDPR (European Union's General Data Protection Regulation), PIPL (The Personal Information Protection Law (PIPL), AND DPDPA, 2023 (Digital Personal Data Protection Act)

[6] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

[7] Javad Pool et al., *A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review*, 74 INT'L J. INFO. MGMT. 102719 (2024), https://doi.org/10.1016/j.ijinfomgt.2023.102719.

[8] Zag ElSayed et al., *Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions*, ARXIV (Jan. 20, 2025), https://arxiv.org/abs/2501.11250.

[9] Lu Zhou et al., *Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities*, 80 J. INFO. SEC. & APPL. 103678 (2024), https://doi.org/10.1016/j.jisa.2023.103678.

3.1. GDPR and AI Regulation

GDPR established major regulatory standards that govern EU processing procedures for Artificial Intelligence systems and biometric information. The **EU AI Act plans**[10] to establish categories of AI systems based on risk exposure followed by requirements for high-risk applications to comply with prescribed regulations. The GDPR establishes clear regulations about AI-powered decision transparency thus it provides individuals with the power to challenge automated decisions.

EU data governance policies regarding AI apply GDPR principles to enforce minimal data handling and specific consent requirements together with limitation of data usage purposes. The upcoming **EU Artificial Intelligence Act** implements risk-based system categories for AI development so regulators determine inspection levels according to AI system threats against basic rights and safety elements.

Under GDPR regulations automated profiling together with behavioral tracking must be constrained to strict limitations which restrict the way companies exploit AI for targeted advertising.[11] The EU has enforced fines on tech corporations for AI-based privacy breaches throughout the latest years which demonstrates that regulatory adherence plays a vital role in AI system implementation.

3.2. China's PIPL and Emerging Technologies

State control together with cybersecurity functions as the core framework that shapes China's governance of artificial intelligence and its related data platform. The Personal Information Protection Law (PIPL) as well as the Data Security Law serve China's intention to maintain state oversight of national data and sensitive or critical information. Chinese AI-system governance follows guidelines which emphasize openness of algorithms and social responsibility while ensuring compliance with socialist principles. The Chinese government preserves its capability to access data for national security reasons yet promotes innovation up to state-defined boundaries. It controls AI processing activities and demands state supervision of personal data management. The Personal Information Protection Law of China targets AI-based profiling and data usage while dealing with worldwide concerns about privacy breaches found in Chinese surveillance systems.[12] Companies operating in China must follow guidelines set by state authorities which require them to present disabled options for AI recommendation systems to their users. The major use of artificial intelligence by China for social credit scoring and surveillance continues to be a point of intense debate in international discussions regarding data protection.

3.3 India's DPDP Act and AI Governance

India upholds a flexible approach to AI governance that promotes innovation development alongside the construction of its nationwide AI governance system. India understands the substantial impact potential of AI in agriculture along with healthcare and education sectors so it established its National AI Strategy as an initiative.[13] The lack of obligatory regulations regarding AI has created uncertainties regarding data privacy standards and obligations for accountable practices. The Act being very new offers global-level protection principles while purpose limitation and storage limitation and lawful processing remain to be operationalized fully in AI systems.

The Digital Personal Data Protection (DPDP) Act of India contains governance provisions for Artificial Intelligence but does not provide specific rules about biometric data processing. Since the Digital Personal Data Protection Act provides exceptions for government surveillance some analysts believe this could reduce the security of AI-based data processing systems. Through its provisions the DPDPA imposes requirements on data fiduciaries which demand AI-powered platforms to deliver non-discriminatory and fair personal data processing. The bill shows weaknesses in privacy protection because it lacks well-defined processes to enforce regulations concerning AI usage.

---

[10] European Parliament, *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARL. (June 1, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[11] Eline Chivot & Daniel Castro, *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy*, CTR. DATA INNOVATION (May 13, 2019), available at https://www2.datainnovation.org/2019-reform-the-gdpr-ai-a4.pdf.

[12] Matt Sheehan, *China's AI Regulations and How They Get Made*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 10, 2023), https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en.

[13] NITI Aayog, *National Strategy for Artificial Intelligence*, GOV'T OF INDIA (Mar. 2023), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

4. PRIVACY-PRESERVING TECHNOLOGIES

With data-intensive technologies such as Artificial Intelligence (AI), Internet of Things (IoT), and Blockchain reshaping digital ecosystems, the protection of privacy for an individual has also become a major issue for governments, organizations, and society. The traditional security mechanisms are becoming ineffective in answering the size, pace, and complexity of data flows within the emerging technologies.

In the era of digital when data has emerged as the most valuable asset, privacy of personal information has become a basic facet of national as well as global legal systems. Privacy-Preserving Technologies (PPTs) development is destined to alleviate the tension between data innovation and legal compliance. These technologies are part of the key developments that are assisting organizations and governments to meet regulatory requirements under devices such as the General Data Protection Regulation **(GDPR),** India's Digital Personal Data Protection Act **(DPDPA),** China's Personal Information Protection Law **(PIPL),** and sector-specific laws like the **Health Insurance Portability and Accountability Act (HIPAA)**. This part studies PPTS of great importance in a legal context.

4.1 Federated Learning

The distributed training mechanism known as federated learning lets devices operate AI models to build knowledge on numerous isolated systems without sharing actual information which boosts protection. The use of this method generates maximum benefit in industries including healthcare and finance because it safeguards vital sensitive information.
This architecture is of legal importance because it reduces the risk of breaching the laws around data localization and the restriction of cross-border data movements, as illustrated in the GDPR **(Art. 44–50)**[14] and the Cybersecurity Law of China.

From the legal compliance standpoint, FL: Minimizes liability risk on data protection laws by storing personal date in local devices. Provides support to the aspects of data minimization and purpose limitation as stipulated by ***Article 5(1)(c) and (b)***[15] *of the GDPR*. Reduces the risks of breaches and conforms to the "privacy by design and default" principles **(GDPR Art. 25)**[16]**.** In healthcare and finance, FL is especially effective because of a stricter level of compliance when such sensitive personal data is being processed (e.g., health records or financial behavior). Its decentralized model also aligns with the maintenance of the right to the portability of data according to **GDPR (Art.20)**[17]**,** because models are able to adapt to local data without any central processing.

Though, FL introduces legal gray areas – like the question of who's the controller vs the processor in distributed systems, and whether we could still indirectly leak sensitive information when aggregating model updates.

4.2 Homomorphic Encryption

Secure data processing through this encryption technique operates without showing the actual data contents which makes it suitable for blockchain applications in addition to secure AI systems. The application of homomorphic encryption shows growing interest for protecting confidential data in cloud systems while enabling international data exchange.

Enhances adherence on principles of data security and confidentiality under such Laws as **GDPR (Art.32), DPDPA Sec. 8 and HIPAA'S Security Rule.** Enables secure international data flows that is consistent with concerns in data transfer adequate assessments as under the **Schrems II.**[18] Allows for meeting requirements on notification of breaches **(GDPR Art. 33)**[19] because, when encrypted, data will not necessarily lead to mandatory breach reporting if key is secure.

[14] GDPR-Info.eu. (n.d.). n.d., Art. 44-50 *General Data Protection Regulation (GDPR)*. Retrieved Feb 18, 2025, from https://gdpr-info.eu
[15] Ibid., Art 5
[16] Ibid., Art 25
[17] Ibid., Art 20
[18] AI-Act-Law.eu. (n.d.). *EU Artificial Intelligence Act*. Retrieved Feb 18, 2025, from https://ai-act-law.eu
[19] Supra note 14

4.3 Zero-Knowledge Proofs (ZKPs)

ZKPs provide users with the capability to demonstrate knowledge about confidential data points without disclosing the actual data contents which improves blockchain transaction privacy. The technological advancement shows growing popularity for use in systems that verify identities together with decentralized financial tools.

Improving anonymity and selective disclosure, compliance with **GDPR Recital 26** and the right to be **forgotten (Art. 17).** Enabling identity verification systems that adhere to the anti-money laundering **(AML)** and know-your-customer **(KYC)** laws but do not collect an excessive amount of personal data. Enabling pseudonymity of decentralized applications (dApps) that might comply with the data minimization principle of the data protection frameworks.

4.4 Differential Privacy

The combination of differential privacy techniques with dataset mathematical noise enables organizations to study trends in anonymized fashion. Tech organizations use this process frequently to protect the anonymity of extensive datasets. It is in line with pseudonymization and anonymization principles from **GDPR Recitals 26 and 29.** May exempt data processors from actually enacting full compliance with data subject rights provided that data sets are actually anonymized-though often subject to the disagreably unclear legal standard of re-identification. Permits observance of exemptions to processing statistical data according to national data protection laws such as **Section 13 of India's DPDPA, 2023.**[20]

5. GOVERNANCE OF EMERGING TECHNOLOGIES IN RELATION TO DATA PROTECTION

5.1 Ethical AI Principles

Government entities as well as industrial leaders work together to set down ethical principles which will govern AI systems. AI systems must maintain fairness together with accountability and transparency according to both the OECD AI Principles and the G20 AI Framework.[21] Ethical AI frameworks need to be uniformly adopted because they protect the principles of human rights and privacy during AI development.

5.2 IoT Security Standards

The ***NIST IoT Cybersecurity Framework as a global initiative*** offers recommended practices to protect IoT devices and network systems.[22] A primary cybersecurity challenge in global security practice involves enforcing uniform security guidelines for IoT manufacturers.

5.3 Regulatory Sandboxes

Aging technologies now undergo testing through controlled regulatory environments before deployment in the UK and Singapore. These programs enable businesses to develop new solutions but do so while protecting their compliance with altering data protection requirements.

5.4 Cross-Border Data Governance

The dual characteristics of frontier technology to transcend borders have created a need for international collaboration on data regulatory policies. *The G7 Data Free Flow with Trust Initiative supports worldwide secure data* sharing activities through collaborative programs that protect individual privacy rights.[23]

The inherent cross-border nature of the frontier technologies (such as AI, IoT, Blockchain) has triggered the development of cross-border data governance models. Such technologies are constantly producing,

[20] Digital Personal Data Protection Act, No. 22 of 2023, § 13, Acts of Parliament, 2023 (India), https://prsindia.org/files/bills_acts/bills_parliament/2023/DPDP_Act_2023.pdf

[21] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence*, OECD.AI (2019), https://oecd.ai/en/ai-principles

[22] INSTAR Standards, *NIST Cybersecurity Framework Version 2.0: Milestone in Global Cybersecurity Standards*, INSTAR STANDARDS (Mar. 26, 2022), https://instarstandards.org/news/nist-cybersecurity-framework-version-20-milestone-global-cybersecurity-standards

[23] World Economic Forum, *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows*, WORLD ECON. F. (2021), https://www.weforum.org/publications/from-fragmentation-to-coordination-the-case-for-an-institutional-mechanism-for-cross-border-data-flows/.

processing, and transferring huge amounts of data across jurisdictions with a disregard of territorial boundaries. Consequently, the national data regulations, in their own application, are not sufficient enough to deal with flow of information worldwide causing tensions within states, and regulatory loopholes as well as threat to individual rights. Such regulatory disintegration leads to **"data sovereignty conflicts"** whereby nations want to dot the **i's** when it comes to data originating in their countries, and in most cases dictates the construction of digital borders. Such barriers can be the barrier to the free flow of data, thus blocking global research collaboration, supply chain integration, and even the interoperability of AI and IoT systems. G7 countries Data Free Flow with Trust (DFFT) Initiative To solve the above challenges, the Initiative – which was first introduced at the **G20 Osaka Summit in 2019**[24] and then brought further by the G7 insists upon the development of a global data governance framework based on confidence, transparency, and shared democratic values.[25] Essentially, the guiding principle of DFFT is the facilitation of free and secure flows on data across the borders while at the same time ensuring that the flows are well protected by strong guarantees and in line with human rights. The DFFT framework has four pillars on which it is based.

1. **Lawful Access to Data:** Making sure rule of law and international legal standards governing access to personal and corporate data by government are observed.
2. **Data Localization Avoidance:** Frustrating forced unneeded data localization that divides global internet fabric and shackle economies from scaling.
3. **Interoperability of Legal Regimes:** Advocating for compatibilities between various national data protection laws with the aim of lowering compliance friction for the global entities.
4. **Multistakeholder Engagement:** Helping to facilitate inclusive participation from the civil society, academia, and the private sector in forming fair, accountable data ecosystems.

By using this initiative, the member states are advancing to interoperable governance models with respect to digital sovereignty and rights. For instance, the leading advocate for DFFT, Japan, has come up with mechanisms for certifying cross- border data transfer while ensuring high level of data protection. Likewise, the European Union, despite its cautiousness, is discovering partnerships consistent with the GDPR by using *the adequacy decisions* as well as *standard contractual clauses.*

5.5 Challenges and Future Directions

The promising course of DFFT nevertheless implies certain difficulties. Nations such as China and Russia still have data localization and national cybersecurity legislations that are against the open models of data flow. Furthermore, the lack of a binding global data treaty, similar to what is there in trade or environmental law, further dilutes the enforcement mechanisms and consistency in cross-border digital rights protection. For overcoming the barriers, there is already a strong agreement to establish baseline global standards for the cross-border data governance under umbrella organizations such as **OECD** (Organisation for Economic Co-operation and Development)**, G20, WTO** (World Trade Organization)**, and UNESCO** (United Nations Educational, Scientific and Cultural Organization) among others. These standards should preferably be neutral to technology and human-centered and have the ability to change with progressions in data-driven innovation. Long term, the construction of "data diplomacy" shall be essential in developing trust, settling disputes and building for sustainable development in an interconnected world. In doing so, it should include not only the state actors but also transnational tech firms, indigenous data communities, and public interest watchdogs to build an inclusive and pluralistic data governance structure.

6. CONCLUSION

Data governance together with AI and IoT and blockchain technologies creates a developing environment that shows both potential rewards and significant risks. Modern technological convergence will enable heretofore unknown industrial efficiency together with individualized solutions and automated operations. The merging technologies require a new data governance approach that uses an all-encompassing adapted approach across different sectors. New regulatory frameworks need to create solutions that handle particular challenges and moral issues which new technologies bring because of their specific risks such as the need to make algorithms clear and to oversee data ownership and data protection and cybersecurity and data movement between nations. The EU establishes its data governance system based on human rights and privacy standards which

[24] "Global Cross-Border Privacy Rules Declaration," Department of Commerce, https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[25] Jennifer Daskal and Debrae Kennedy-Mayo, "Budapest Convention: What is it and how is it being updated" (Cross-Border Data Forum, July 2, 2020), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

includes tight regulations for innovation purposes. National security and state control remain as the core principles of China's model which enables administrators to maintain governance over new technologies. India follows a dual strategy which strives to unify national economic targets with democratic principles and data protection policies. These three distinct geographic areas display distinctive methods through which countries handle innovation and regulatory demands during the digital period.

The development of AI, IoT and blockchain requires policymakers to establish proper equilibrium between technological progression and information security mechanisms. The era of emerging technologies requires international partnerships between authorities and robust regulatory systems and privacy-preserving technologies to establish responsible data governance. Data protection in upcoming years will succeed through proper management of the intricate connection between technological development and privacy rights by both governments and businesses together with civil society.

REFERENCES

[1] Joshi, Navmi. (2024). Emerging Challenges in Privacy Protection with Advancements in Artificial Intelligence. International Journal of Law and Policy 2. 55-77. 10.59022/ijlp.171.

[2] ACLU v. Clearview Ai, Inc., 2021 Ill. Cir. LEXIS 292 DePaul University, *Journal of Art, Technology, and Intellectual Property*, DEP. UNIV. (2025), https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1651&context=jatip.

[3] Zag ElSayed et al., *Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions*, ARXIV (Jan. 20, 2025), https://arxiv.org/abs/2501.11250.

[4] Lawfare, *Human Subjects Protection in the Era of Deepfakes*, LAWFARE (Nov. 2, 2023), https://www.lawfaremedia.org/article/human-subjects-protection-in-the-era-of-deepfakes.

[5] Cloud Security Alliance, *Amazon Ring: A Case of Data Security and Privacy*, CSA (Mar. 26, 2022), https://cloudsecurityalliance.org/blog/2022/03/26/amazon-ring-a-case-of-data-security-and-privacy.

[6] Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117

[7] Javad Pool et al., *A Systematic Analysis of Failures in Protecting Personal Health Data: A Scoping Review*, 74 INT'L J. INFO. MGMT. 102719 (2024), https://doi.org/10.1016/j.ijinfomgt.2023.102719.

[8] Zag ElSayed et al., *Cybersecurity and Frequent Cyber Attacks on IoT Devices in Healthcare: Issues and Solutions*, ARXIV (Jan. 20, 2025), https://arxiv.org/abs/2501.11250.

[9] Lu Zhou et al., *Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities*, 80 J. INFO. SEC. & APPL. 103678 (2024), https://doi.org/10.1016/j.jisa.2023.103678.

[10] European Parliament, *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARL. (June 1, 2023), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

[11] Eline Chivot & Daniel Castro, *The EU Needs to Reform the GDPR to Remain Competitive in the Algorithmic Economy*, CTR. DATA INNOVATION (May 13, 2019), available at https://www2.datainnovation.org/2019-reform-the-gdpr-ai-a4.pdf.

[12] Matt Sheehan, *China's AI Regulations and How They Get Made*, CARNEGIE ENDOWMENT FOR INT'L PEACE (July 10, 2023), https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en.

[13] NITI Aayog, *National Strategy for Artificial Intelligence*, GOV'T OF INDIA (Mar. 2023), https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf.

[14] Organisation for Economic Co-operation and Development (OECD), *OECD Principles on Artificial Intelligence*, OECD.AI (2019), https://oecd.ai/en/ai-principles

[15] GDPR-Info.eu. (n.d.). n.d., Art. 44-50 *General Data Protection Regulation (GDPR)*. Retrieved Feb 18, 2025, from https://gdpr-info.eu

[16] Ibid., Art 5

[17] Ibid., Art 25

[18] Ibid., Art 20

[19] AI-Act-Law.eu. (n.d.). *EU Artificial Intelligence Act*. Retrieved Feb 18, 2025, from https://ai-act-law.eu

[20] Supra note 14

[21] Digital Personal Data Protection Act, No. 22 of 2023, § 13, Acts of Parliament, 2023 (India), https://prsindia.org/files/bills_acts/bills_parliament/2023/DPDP_Act_2023.pdf

[22] INSTAR Standards, *NIST Cybersecurity Framework Version 2.0: Milestone in Global Cybersecurity Standards*, INSTAR STANDARDS (Mar. 26, 2022), https://instarstandards.org/news/nist-cybersecurity-framework-version-20-milestone-global-cybersecurity-standards

[23] World Economic Forum, *From Fragmentation to Coordination: The Case for an Institutional Mechanism for Cross-Border Data Flows*, WORLD ECON. F. (2021), https://www.weforum.org/publications/from-fragmentation-to-coordination-the-case-for-an-institutional-mechanism-for-cross-border-data-flows/.

[24] "Global Cross-Border Privacy Rules Declaration," Department of Commerce, https://www.commerce.gov/global-cross-border-privacy-rules-declaration

[25] Jennifer Daskal and Debrae Kennedy-Mayo, "Budapest Convention: What is it and how is it being updated" (Cross-Border Data Forum, July 2, 2020), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.