

ARTIFICIAL INTELLIGENCE AND DIGITAL DOMINANCE:

Shaping the Future World Order



Editors

Dr. B. Indira Priyadharshini

Dr. M. Deepa

Dr. M. Shanmuga Priya

Dr. R. Ramya

ARTIFICIAL INTELLIGENCE AND DIGITAL DOMINANCE: SHAPING THE FUTURE WORLD ORDER

EDITORS

Dr. B. Indira Priyadharshini | Dr. M. Deepa

Dr. M. Shanmuga Priya | Dr. R. Ramya

Assistant Professors

UG Department of Commerce (CA)

NGM College, Pollachi.

ARTIFICIAL INTELLIGENCE AND DIGITAL DOMINANCE: SHAPING THE FUTURE WORLD ORDER

© **Dr. B. Indira Priyadharshini**
Dr. M. Deepa
Dr. M. Shanmuga Priya
Dr. R. Ramya

First Edition: July, 2026.

ISBN: 978-93-5987-439-5

Price: Rs. 0.00/-

Copyright

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted. In any form or by any means, mechanical, photocopying, recording or otherwise, without prior written permission of the author.

Printed at

SHANLAX PUBLICATIONS

61, 66 T.P.K. Main Road

Vasanthanagar

Madurai - 625003

Tamil Nadu, India

Ph: 0452-4208765

Mobile: 7639303383

email: publisher@shanlaxpublications.com

web: www.shanlaxpublications.com

28.	Artificial Intelligence in Accounting and Finance: Opportunities, Challenges, and Ethical Implications for India's Digital Economy Ms. V. Poornima	190
29.	India's National AI Strategy and Global Competitiveness Dr. D. Rajasekaran & Ms. P.M. Sri Raja Mahalakshmi	198
30.	AI Surveillance and its Impact on Global Power Structure P. Anitha	203
31.	Digital Economy and Global Trade in the New World Order K. Abirami & A. Sindhupriya	207
32.	An Empirical Study on the Role of Insurance Companies in Promoting Environmentally Aligned Growth through Green Finance and Green Accounting Ms. Gomathi A	213
33.	Fin Tech Innovation and Digital Payments in International Trade: Opportunities, Challenges, and Implications for Global Economic Growth in the Digital Economy Dr. S. Shanmugapriya & Ms. V. Brintha	222
34.	India's Emerging Role in Democratic Technology Governance: Opportunities and Challenges Dr. R. Kalaiselvi	229
35.	Artificial Intelligence Adoption and India's Digital Economy: Opportunities, Cybersecurity Challenges, and Policy Implications in the New World Order Dr. Vishalakshi, Supriya. R & Navisha. R	233
36.	Ethical, Legal, and Social Implications of Artificial Intelligence in the Era of Digital Dominance: A Global and Indian Perspective Dr. N. Bagyalakshmi	239
37.	Performance Assessment of Deep Belief Networks Using AI Techniques Dr. A. Kalaivani & Dr. R. Jayaprakash	250
38.	AI and Geopolitics Reshaping International Power and Strategic Competition Dr. G. Vignesh & Ms. B. Sri Durga	268
39.	Artificial Intelligence and the future of Digital Diplomacy Ms. G.Gayathri	274
40.	Artificial Intelligence As a Driver of the New World Order Dr. M. Prem & S. Meenakshi	280
41.	Challenges in Data Governance, Privacy, and Digital Sovereignty Mrs. M. Ragaprabha & Mohan Raj. V	283
42.	Cyber Laws, Regulations, and Global Governance Frameworks Dr. M. Prem & G. Jeevanantham	289
43.	Digital Diplomacy and International Relation Mr . M. Prem & G.Arish	292

CHALLENGES IN DATA GOVERNANCE, PRIVACY, AND DIGITAL SOVEREIGNTY

Mrs. M. Ragaprabha

Assistant Professor

PG Department of Commerce with International Business

NGM College, Pollachi

Mohan Raj. V (25-PI-13)

II M.Com IB

PG Department of Commerce with International Business

NGM College, Pollachi

Abstract

Data Governance, Privacy, and Digital Sovereignty have become essential components of the digital era. Effective data governance ensures the proper collection, management, security, and utilization of data while maintaining transparency and accountability. Privacy focuses on protecting individuals' personal information and safeguarding their rights against unauthorized access and misuse. Digital sovereignty refers to a nation's ability to control and regulate its digital infrastructure, data, and technologies in accordance with its laws and national interests. Together, these concepts play a crucial role in promoting cybersecurity, building public trust, ensuring regulatory compliance, and strengthening economic and national security. As digital technologies continue to evolve, balancing innovation with privacy protection and sovereign control remains a key challenge for governments, organizations, and societies world wide.

Keywords: *Challenges, Data Governance, Privacy, Digital Sovereignty.*

Introduction:

In the digital age, data has become a valuable resource that drives economic growth, innovation, and technological advancement. As the volume of digital information continues to increase, the need for effective data governance, privacy protection, and digital sovereignty has become increasingly important. Data governance ensures that data is collected, managed, and used responsibly through appropriate policies and regulations. Privacy focuses on safeguarding individuals' personal information and protecting their rights from unauthorized access and misuse. Digital sovereignty refers to a nation's ability to control its digital infrastructure, data, and technologies in accordance with its laws and strategic interests. Together, these concepts help strengthen cybersecurity, build public trust, promote responsible data management, and support national security and economic development in an increasingly interconnected world.

Objectives:

- To establish a structured framework for managing data accurately, securely, and responsibly throughout its lifecycle.
- To protect personal and sensitive information by ensuring privacy, confidentiality, and compliance with applicable laws and regulations.

- To strengthen digital sovereignty by enabling organizations and nations to retain control over their data, digital infrastructure, and technology resources.

Privacy

Privacy refers to the protection of individuals' personal data and the right to control how their information is collected, stored, processed, and shared. It is a key component of data governance, ensuring that personal information is handled securely, ethically, and in compliance with privacy laws. Strong privacy practices help prevent unauthorized access, reduce the risk of data breaches, and build trust in digital systems.

Data Governance

Data Governance is the process of managing data to ensure it is accurate, secure, consistent, and accessible. It establishes policies, standards, and responsibilities for collecting, storing, using, and sharing data. Effective data governance improves data quality, supports better decision-making, ensures compliance with laws and regulations, and protects sensitive information from unauthorized access.

Digital Sovereignty

Digital Sovereignty is the ability of a country or organization to control and manage its digital data, technologies, and digital infrastructure according to its own laws and policies. It helps protect national security, ensures data privacy, reduces dependence on foreign technology, and gives greater control over how data is stored, processed, and shared.

Cybersecurity

Cybersecurity is the practice of protecting computers, networks, systems, and data from cyberattacks, unauthorized access, theft, and damage. It uses technologies, policies, and security measures such as firewalls, encryption, antivirus software, and strong passwords to keep information safe. Effective cybersecurity helps protect privacy, maintain business continuity, and ensure the confidentiality, integrity, and availability of data.

Regulatory Compliance

Regulatory Compliance is the process of ensuring that an organization follows all applicable laws, regulations, standards, and policies related to its operations. It helps protect customer data, reduces legal and financial risks, promotes ethical business practices, and builds trust with customers and stakeholders.

Data Quality

Data Quality refers to the accuracy, completeness, consistency, reliability, and timeliness of data used within an organization. High-quality data ensures that information is correct, up to date, and fit for its intended purpose. It supports better decision-making, improves operational efficiency, enhances customer trust, and helps organizations comply with regulatory requirements. Maintaining data quality involves regular validation, cleansing, monitoring, and updating of data to minimize errors and inconsistencies.

Data Integrity

Data Integrity refers to the accuracy, consistency, completeness, and reliability of data throughout its entire lifecycle. It ensures that data remains unchanged, correct, and protected from unauthorized modification, corruption, or loss. Maintaining data integrity is essential for trustworthy decision-making, regulatory compliance, and secure information management. Organizations achieve data integrity through validation, access controls, encryption, backups, and regular audits.

Risk Management

Risk Management is the process of identifying, assessing, and controlling risks that may affect an organization's data, systems, and operations. It helps minimize threats such as cyberattacks, data breaches, system failures, and regulatory violations. Effective risk management involves evaluating potential risks, implementing security controls, monitoring vulnerabilities, and developing response plans. This process protects valuable information, ensures business continuity, and supports compliance with legal and regulatory requirements.

Methodology

The methodology for Data Governance, Privacy, and Digital Sovereignty begins with identifying and classifying organizational data based on its sensitivity and importance. Clear governance policies are then established to define how data is collected, stored, accessed, shared, and disposed of. Privacy is ensured by implementing measures such as informed consent, encryption, access controls, and data minimization to protect personal information. Digital sovereignty is maintained by storing and processing critical data in accordance with national laws and regulatory requirements, ensuring that organizations retain control over their digital assets. Regular risk assessments, security monitoring, compliance audits, and employee training help identify vulnerabilities and strengthen data protection practices. Finally, the governance framework is continuously reviewed and updated to address emerging technologies, evolving cyber threats, and changing legal requirements, ensuring secure, transparent, and responsible data management.

Major Challenges in Data Governance, Privacy, and Digital Sovereignty

- **Data Security Threats:**

One of the most critical challenges in data governance is the increasing frequency of cyber attacks and data breaches. Organizations store vast amounts of sensitive information, including financial records, health data, and personal identities. Cybercriminals exploit vulnerabilities in networks, cloud systems, and applications to gain unauthorized access. Data breaches can result in substantial financial losses, reputational damage, legal penalties, and loss of customer trust. For governments, compromised data can pose risks to national security and public administration. Consequently, strengthening cyber security measures has become a fundamental requirement of effective data governance.

- **Privacy Concerns**

The widespread collection and processing of personal data by social media platforms, e-commerce companies, and digital service providers have raised serious privacy concerns. Individuals often share information without fully understanding how it will be used, stored, or shared with third parties. Excessive data collection may lead to surveillance, profiling, identity theft, and unauthorized exploitation of personal information. Protecting privacy requires clear consent mechanisms, transparent data practices, and strong legal safeguards that give individuals greater control over their personal data.

- **Lack of Uniform Regulations**

Different countries have adopted different data protection laws and regulatory standards. For example, the European Union's General Data Protection Regulation (GDPR) establishes strict requirements for data processing and user consent, while other countries follow different approaches. Multinational organizations operating across several jurisdictions must comply with multiple legal frameworks, increasing compliance costs and administrative complexity. The absence of harmonized international regulations creates uncertainty regarding data handling, enforcement, and accountability.

- **Cross-Border Data Flows**

Digital services often involve the transfer of data across national borders through cloud computing and global digital networks. Data generated in one country may be stored or processed in another, creating challenges related to jurisdiction and legal control. Conflicting national laws may affect access to data, law enforcement cooperation, and security requirements. Managing cross-border data flows requires international agreements and collaborative mechanisms that balance economic efficiency with privacy and security concerns.

- **Rapid Technological Advancements**

Technologies such as artificial intelligence, big data analytics, block chain, cloud computing, and the Internet of Things are evolving at a pace that often exceeds regulatory development. New technologies create novel methods of collecting, analyzing, and monetizing data. Regulators frequently struggle to update legal frameworks quickly enough to address emerging risks. This regulatory lag can create gaps in oversight, unclear accountability, and increased exposure to privacy and ethical challenges.

- **Balancing Innovation and Regulation**

Governments face the difficult task of encouraging technological innovation while protecting citizens' rights. Excessive regulation may discourage investment, research, and digital entrepreneurship. Conversely, weak regulation can expose individuals and organizations to significant privacy and security risks. An effective policy framework should promote responsible innovation by establishing clear standards for data protection without creating unnecessary barriers to technological progress.

- **Digital Dependence on Foreign Technologies**

Many countries depend heavily on foreign digital platforms, cloud providers, software systems, and communication infrastructure. This dependence can limit a nation's ability to control critical digital resources and protect strategic interests. Geopolitical tensions may affect access to technologies, digital services, and data infrastructure. Strengthening domestic technological capabilities has therefore become an important component of digital sovereignty strategies.

- **Data Localization Challenges**

Data localization policies require certain categories of data to be stored within a country's borders. While localization may enhance governmental oversight and security, it can also increase operational costs for businesses and reduce the efficiency of global cloud services. Organizations may need to establish local data centers and modify their digital infrastructure to comply with national requirements. These measures can affect international digital trade and cross-border business operations.

- **Lack of Public Awareness**

A significant challenge is the limited awareness among individuals and organizations regarding data protection practices and cyber risks. Many users do not fully understand privacy settings, phishing threats, or the implications of sharing personal information online. Small and medium-sized enterprises often lack adequate cyber security training and resources. Improving digital literacy and public awareness is essential for creating a stronger culture of data protection.

- **Ethical Issues and Accountability**

The increasing use of data-driven technologies raises important ethical questions. Artificial intelligence systems may produce biased outcomes that affect employment, credit approval, healthcare access, and public services. Ensuring transparency, fairness, and accountability in automated decision-making is a major challenge. Organizations must establish ethical guidelines and governance mechanisms to prevent discrimination and misuse of data.

Conclusion:

Data governance, privacy, and digital sovereignty are increasingly important in shaping a secure and resilient digital future. Effective governance frameworks ensure the responsible collection, management, and use of data, while strong privacy measures protect individual rights and enhance public trust. Digital sovereignty enables countries to maintain control over their digital infrastructure and strategic data resources. Although challenges such as cybersecurity threats, regulatory differences, and technological dependence persist, emerging developments in artificial intelligence, privacy-enhancing technologies, and sovereign digital infrastructure offer new opportunities for strengthening digital ecosystems. Therefore, achieving a balance between innovation,

security, privacy, and national interests is essential for sustainable economic growth, technological advancement, and long-term digital resilience in an interconnected world.

References:

1. Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press.
2. Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.
3. Greenleaf, G. (2021). *Global Data Privacy Laws and Their Impact on International Business*. Edward Elgar Publishing.
4. World Economic Forum. (2023). *Global Risks Report 2023*. Geneva: World Economic Forum.
5. Organisation for Economic Co-operation and Development (OECD). (2020). *OECD Digital Economy Outlook 2020*. Paris: OECD Publishing.