





Book Review: Understanding Cybersecurity Law in Data Sovereignty and Digital Governance by Melissa Lukings and Arash Habibi Lashkari

Aftab Haider ^{1*} and Jamil Afzal ²

¹Abdul Wali Khan University Mardan, Pakistan

²International Islamic University Malaysia

* Corresponding Email: jamilafzal@iium.edu.my

Received: 10 March 2025 / Revised: 25 April 2025 / Accepted: 21 May 2025 / Published online: 11 June 2025

This is an Open Access article published under the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). © International Journal of Law and Legal Advancement (IJLLA) published by SCOPUA (Scientific Collaborative Online Publishing Universal Academy). SCOPUA stands neutral with regard to jurisdictional claims in the published maps and institutional affiliations.

Melissa Lukings and Arash Habibi Lashkari are authors of the book “Understanding Cybersecurity Law in Data Sovereignty and Digital Governance.” It provides a comprehensive analysis of the intersection between law, cybersecurity, and data sovereignty in the digital age. The best readers for this book are legal and policy experts, IT professionals, and people who want to learn about data privacy governance and security laws (Lukings & Lashkari, 2022). In **Chapter 1**, the authors explain *data sovereignty*, which means data must follow the rules of the country that collects it. Data sovereignty challenges the idea that a country's control is only linked to its geographic borders. The chapter explains how data functions as a legal element and highlights its relationship with security controls for personal information and cloud storage systems. Data sovereignty is important because digital information often crosses international borders (Afzal, 2024). On pages **1-7**, the authors use Canada's data sovereignty framework as a key example to illustrate how the country maintains control over its digital information. The chapters on data management explain the rules surrounding data residency and localization (pages **7-15**). The chapter explores how states influence digital data storage rules, highlighting the legal challenges of cross-border cloud computing. The authors show how governments and companies must handle data security challenges when managing international data operations (pages **16-17**).

In **Chapter 2, *Digital Governance***, Melissa Lukings, and Arash Habibi Lashkari look at how governance practices are changing as more activities move online. They examine various leadership systems that ensure clear accountability. These systems promote open information sharing and encourage community engagement, benefiting both governments and businesses. The chapter demonstrates how technology empowers citizens and enhances institutional performance while introducing new security challenges. Digital technologies create several problems, including government corruption and unaccountability, along with inadequate digital technology use. The authors show how digital companies must balance making money with taking care of society by following ethical rules. Digital governance gives many advantages but needs defined laws to stop unfair use in digital areas (pages **39-60**). The chapter organizes content around key governance standards, such as social responsibility, accountability, and transparency. The authors explain why social contracts remain essential for digital governance to win public confidence and online institution credibility. The chapter studies how user-generated content affects company responsibility and explains the legal complications when handling such content (pages **61- 79**). The key part of this chapter shows how digital technology lets people take control, but it also creates new governance issues when these tools move faster than legal systems can handle (pages **79-81**).

Chapter 3 focuses on conflicts of law and explains how jurisdictions handle legal matters that span international borders. It focuses on how legal systems handle cases with connections to different jurisdictions. The chapter explains how to establish legal authority between different countries and within domestic borders at both national and international levels. The authors examine how personal characteristics such as nationality and living status reveal which country's laws should apply (pages **85-95**). The authors clarify how prescriptive enforcement and adjudicative jurisdictions work across borders when addressing cybercrimes and international conflicts. Both international law and different legal systems within countries get in-depth exploration together with methods to handle legal system clashes. The authors discuss how it is becoming more difficult to define rules for cyberspace. This is because criminal investigations and online defamation cases often involve multiple countries (pages **100-110**).

In **Chapter 4, *Technical Complexities***, the authors discuss the complex challenges arising from the intersection of law, technology, and governance in the digital age. New technology brings complicated challenges for managing data legally and ethically. This study examines the growth of big data and addresses issues such as ownership of corporate and government data, security risks associated with metadata, and the occurrence of data breaches (pages **117-123**). Data plays a crucial role in today's society. It affects healthcare and how people connect. Because of this, we need effective laws to protect user data now. People



recognize how valuable their data is, which has led to more laws aimed at keeping it safe. Despite new laws, governments face difficulties protecting user rights because companies store data across multiple countries. The authors show how international data storage makes it hard for countries to enforce their data protection rules (pages **118-127**). The authors detect essential privacy risks from data vault developments and metadata problems through their crucial review. As cloud computing becomes more prevalent, shared data networks may lead to data breaches affecting millions globally (pages **123-126**). This chapter talks about how data management confrontations shape internet rules internationally and affect the dilemma between keeping information open and close (pages **128-157**).

Chapter 5 examines the legal frameworks that various countries use to address the increasing concerns around data sovereignty and digital governance. This key chapter shows how different regions handle data management and control according to their national standards and global network connections. According to the authors, data protection strategies in different countries arise from local political conditions and vary in their balance between national security and international interaction (pages **181-200**). The chapter explains that international data rules vary and lack standard definitions. It focuses on two main ideas: data residency and data localization. Data residency involves where data is stored, while data localization requires that sensitive government data stay within the country. The chapter examines both concepts in detail, showing where data is stored around the world and outlining the requirements for data localization. The authors illustrate how governments across Canada, China, and the European Union establish security measures to defend their nations and secure citizen rights (pages **201-220**). The data sovereignty discussion focuses on matters of national security, economic self-defence, and independent tech advancement, as shown by critical assessment. The authors warn that strict data rules could disrupt global data sharing. They emphasize the balance between promoting economic growth and ensuring personal safety. As per the authors, GDPR and similar EU privacy laws help secure personal data, but their data exchange limits may slow business development (pages **220-230**). This chapter explores the ethical issues between businesses collecting user data and citizens seeking privacy. The authors evaluate national data regulation systems to show why international data cooperation must replace these solutions in the long term.

Chapter 6 explores the urgent digital governance problems facing data sovereignty today and explains their impact on our modern digital world. Melissa Lukings and Arash Habibi Lashkari look at barriers to digital rights. They discuss how Indigenous people protect their data and the roles of data centres, artificial intelligence, and data governance ethics. The chapter explains that digital expansion needs rules to defend human rights and make digital platforms socially responsible while handling environmental and global political challenges. They discuss



how digital oppression, data surveillance, and artificial intelligence ethics must be integral parts of any system that governs technology use (pages **265-270**). Digital rights, the main focus of this chapter, are divided into moral and legal categories. These rights allow people to interact with digital content while keeping their privacy safe. They also protect the rights to express oneself and associate with others (pages **271-280**). The authors demonstrate that governments should defend digital rights both by protecting them and by making them practical in online spaces. The authors highlight the APC Internet Rights Charter principles, which show how the Internet enables these fundamental rights and needs (pages **280-290**). The authors strongly focus on Indigenous data control rights through the CARE framework. This chapter explains why Indigenous communities struggle to control their data and how this influences their basic rights. It highlights the need for changes in Western laws to improve Indigenous access to resources and support their self-governance rights (**290-300**). The legal examples of Indigenous sovereignty in Canada show why legal systems need to evolve to defend both Indigenous rights and protect community data from exploitation (pages **300-310**). The authors examine the impacts data centres and data mining have on society and the environment. Data centres are essential for our connected world, but they use a lot of electricity and cause serious environmental issues. The rise of data use and AI technologies can threaten people's basic rights to decide how they use digital tools. The chapter urges companies and governments to uphold ethical principles by regulating how AI and machine learning systems are applied to human rights standards (pages **310-330**). In their final remarks, the authors push for a new approach to digital governance that solves all emerging issues through international collaboration and standard setting (pages **330-340**).

The authors, Melissa Lukings and Arash Habibi Lashkari have undoubtedly provided a thorough and inspiring examination of data sovereignty and digital governance, yet their work raises some critical and interesting questions that demand deeper analysis. **Chapter 1** clearly explains data sovereignty but could have been improved by exploring how different regions around the world define data sovereignty. It should have been discussed how these definitions affect international business. The chapter explains data storage problems with cloud computing but does not fully explore how companies move data across countries to avoid national regulations and create legal conflicts. Countries need to find ways to protect their data from foreign control because digital infrastructure works across borders. Despite useful digital governance insights, **Chapter 2** fails to explain how governance structures will be enforced, especially with emerging technologies like blockchain and decentralized platforms. Do rules for offline systems work on digital platforms without borders, or do we need new leadership methods? They should have looked at how well companies maintain ethical standards beyond their online activities. The authors correctly call for more controls, but they should have



considered whether corporate self-regulation has worked in the past since company profits often conflict with proper conduct. The book examines conflicts of law effectively but misses changes in state jurisdictions over tech companies like Google, Facebook, and Amazon, plus their effects on international legal systems. When international companies open offices in different countries, should those countries follow strong legal systems, or should they create a fair global law network? The **Chapter 4** explanation of technology challenges stands strong while missing key ethical problems arising from fast technology growth, including AI bias and data privacy risks. Companies and governments often use AI technology without assessing its effects on society. The authors should have evaluated this misuse more deeply. Their analysis of data ownership must have looked at who controls personal data across companies, governments, and users since data operates as a market asset instead of serving society. The authors should explain the political challenges that come up when creating data sovereignty laws, especially in countries with weak legal systems. How can States with poor law enforcement and leadership structures follow data sovereignty rules without violating fundamental rights? **Chapter 6** presents important emerging topics but possibly exaggerates their universal impact. The universal nature of issues like AI ethics and digital colonialism demands local context-specific solutions to work successfully across diverse socio-political and legal frameworks. The authors should have recognized that every circumstance demands unique solutions and accepted that different digital governance strategies work best. The authors provided an important addition to professional knowledge through their work. Their study combines law and technology research to explain how data sovereignty interacts with digital rights across different countries. The author's clear writing style and detailed research create a valuable asset for people working in digital governance fields and students pursuing digital policies. The book provides a critique of present digital governance systems while presenting an ethical path to improved digital policies and governance models. We would highly recommend this book to anyone seeking to understand the urgent issues related to cybersecurity, data privacy, and global digital policy.

Declaration

Author Contribution: N/A

Conflict of Study: N/A

Ethical Approval and Consent of Participation: N/A

Funding: This work did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

References

- Afzal, J. (2024). Implementation of digital law as a legal tool in the current digital Era. In: Springer.
- Lukings, M., & Lashkari, A. H. (2022). Understanding cybersecurity law in data sovereignty and digital governance. *Cham: Springer International Publishing*.

Author(s) Bio



Aftab Haider:

A.H. is a practicing lawyer in Pakistan and an International Arbitrator at the Chongqing Arbitration Commission (CQAC), in China. He is currently pursuing his PhD at Southwest University of Political Science and Law, with specialized expertise in transnational organized crimes and international law. Mr. Haider has published over a dozen scholarly articles in internationally recognized journals, covering diverse topics such as organized crime, environmental law, human rights, and international arbitration. He has also contributed as an editor and reviewer for multiple academic journals and actively participates in international legal conferences and workshops. His professional background combines strong legal research, arbitration practice, and cross-border legal cooperation.

Jamil Afzal:

J.A. has been involved in research and teaching for various National and International institutes for more than ten years. He is the author of four books and a contributor/associate editor in two others, along with different high-ranking journal articles; he also participated in various reputed international conferences.

