Chapter 7
Privacy and Security: Safeguarding Personal Data in the AI Era

Geeta Sandeep Nadella
https://orcid.org/0000-0001-7126-5186
University of the Cumberlands, USA

Hari Gonaygunta
https://orcid.org/0009-0003-3360-154X
Department of Information Technology, University of the Cumberlands, USA

Mohan Harish
Department of Information Technology, University of the Cumberlands, USA

Pawan Whig
https://orcid.org/0000-0003-1863-1591
VIPS, India

ABSTRACT

In the rapidly advancing landscape of artificial intelligence (AI), the intersection of privacy and security has emerged as a critical focal point. This chapter explores the multifaceted challenges and considerations involved in safeguarding personal data within the AI era. It delves into the ethical implications of AI-driven data collection, storage, and utilization, emphasizing the importance of privacy-preserving technologies and robust security measures. Through case studies and theoretical frameworks, the chapter examines current practices and future directions aimed at balancing innovation with the protection of individual privacy rights. By addressing these issues, it aims to equip stakeholders—from developers to policymakers—with the knowledge needed to navigate the complex terrain of AI ethics and ensure responsible data stewardship in the digital age.

DOI: 10.4018/979-8-3693-4147-6.ch007

Copyright © 2025, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

In recent years, the rapid advancement of artificial intelligence (AI) has transformed various aspects of society, promising unprecedented opportunities for innovation and efficiency. However, this technological revolution has also brought to the forefront critical concerns regarding privacy and security. As AI systems become more pervasive and integral to daily life—from personalized recommendations on social media to autonomous vehicles—the collection, processing, and utilization of vast amounts of personal data have raised ethical, legal, and societal challenges.

This chapter serves as an exploration into the evolution of privacy and security in the AI era. It begins by tracing the historical context of privacy rights and data protection, highlighting key milestones and regulatory frameworks that have shaped current practices. The chapter then examines the unique implications of AI technologies on these foundational principles, discussing how machine learning algorithms and big data analytics have enabled both new opportunities and risks.

Central to this discussion is the concept of ethical AI development. As AI systems increasingly rely on sensitive personal data to make decisions and predictions, ensuring ethical practices becomes paramount. Issues such as algorithmic bias, transparency, and accountability come to the forefront, necessitating a balanced approach that fosters innovation while safeguarding individual rights. The chapter explores notable examples and case studies where privacy breaches or security vulnerabilities in AI systems have occurred, illustrating real-world implications and lessons learned. It also discusses the role of stakeholders—including governments, technology companies, researchers, and users—in shaping policies and practices that promote responsible AI deployment.

Looking forward, the chapter concludes by outlining emerging trends and innovations aimed at enhancing privacy and security in the AI ecosystem. Topics such as federated learning, differential privacy, and blockchain-based solutions are examined as potential pathways to mitigate risks and protect user data in increasingly complex AI environments. This introduction sets the stage for the subsequent chapters, which delve deeper into specific aspects of privacy and security in the AI era. By providing a comprehensive overview of these foundational issues, the chapter aims to equip readers with a nuanced understanding of the evolving landscape and ethical imperatives surrounding AI technologies.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/privacy-and-security/359642

Related Content

A New View of Privacy in Social Networks: Strengthening Privacy During Propagation

Wei Changand Jie Wu (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 517-541).*

www.irma-international.org/chapter/a-new-view-of-privacy-in-social-networks/228743

Unpacking the Psychological and Social Impact of Deepfake Technology on Students

P. Velavan, P. Sabitha, M. Iswarya, R Thangamani, A. Mohamed Fahadhu, J. Mohamed Zakkariya Maricarand Rahul Chauhan (2026). *Safeguarding Educational Integrity Through Deepfake Face Detection (pp. 169-190).*

www.irma-international.org/chapter/unpacking-the-psychological-and-social-impact-of-deepfake-technology-on-students/398644

The Future of National and International Security on the Internet

Maurice Dawson, Marwan Omar, Jonathan Abramsonand Dustin Bessette (2019). *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications (pp. 1666-1696).*

www.irma-international.org/chapter/the-future-of-national-and-international-security-on-the-internet/228803

AI Ethics in Financial Decision-Making: Accountability, Transparency, and Bias

Nida Fatimahand K. Jayashree (2026). *The Ethical Landscape of AI: Global Issues and Solutions (pp. 383-412).*

www.irma-international.org/chapter/ai-ethics-in-financial-decision-making/399873

Taxonomy of Cyber Threats to Application Security and Applicable Defenses

Winfred Yaokumah, Ferdinard Katsriku, Jamal-Deen Abdulaiand Kwame Okwabi Asante-Offei (2020). *Modern Theories and Practices for Cyber Ethics and Security Compliance (pp. 18-43).*

www.irma-international.org/chapter/taxonomy-of-cyber-threats-to-application-security-and-applicable-defenses/253660