Chapter 8
Navigating the Digital Labyrinth:
Personal Data Privacy and Security at Individual and Organizational Levels

Md Mehedi Hasan Emon
https://orcid.org/0000-0002-6224-9552
American International University-Bangladesh, Bangladesh

ABSTRACT

This chapter critically examines the evolving landscape of personal data privacy and security amid rapid digital transformation. It explores the multifaceted challenges faced by individuals and organizations, including asymmetries in data control, cyber vulnerabilities, and systemic governance failures. The chapter provides a comprehensive overview of global regulatory frameworks such as the GDPR, CCPA, and emerging policies in the Global South, highlighting both progress and persistent compliance gaps. Emphasis is placed on best practices risk assessments, employee training, incident response, and data minimization as well as the role of cutting-edge technologies like AI, blockchain, and encryption in strengthening data protection. Ultimately, the chapter underscores the necessity of cultivating a security-oriented culture that embeds privacy into organizational ethos, urging a shift from reactive compliance to proactive responsibility in managing digital trust.

DOI: 10.4018/979-8-3373-3171-3.ch008

INTRODUCTION

As digitalization, that is the interconnection of cities, businesses and peoples for the modern era, becomes more and more prevalent in today's world, the issue centering around personal information is of fundamental importance. The purpose of this chapter is to define the dynamic and complex body of personal data privacy and security as both individual and corporate. The title references the complexity and fluidity of efforts to shelter information in the coming generations of invisible and living political technology, where legal movements adapt to fast-paced technical and social technological movements. The chapter starts with putting emphasis on how urgent the issue is by understanding it through the prism of digital change. Although such digitalization is efficient, convenient and provides, at the same time, the possibility to innovate, it also exposes the individuals and businesses to new risks like identity theft, surveillance, harm to reputation, and legal liability. The contribution of this chapter consists in the critical analysis of four empirical examples and real-world case studies that show that data security breaches do not rely on technical errors only but are also signs of impassable organizational, ethical, and structural deficiencies. In the following sections, the main challenges to both individuals and institutions are addressed: lack of access to information, weak governance frameworks, and human-centric weakness. Next, discourse moves on to discuss the subject of international regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in terms of their scope, efficiency, and limitations that arise for companies to remain compliant in distinct jurisdictions. Therefore, the chapter takes care to note that a mere legal compliance is not enough and recommends a set of best practices that seek to increase data privacy using proactive organizational strategies. These encompass personnel training, ongoing risk evaluation, and comprehensive incident response planning. I also make particular emphasis on the future technologies blockchain, encryption protocols, and artificial intelligence—as both future remedies and the causes of new kinds of ethical struggles. The chapter finishes with the discussion that technology and policy must nexus with a general corporate culture of responsibility, mindfulness, and caution. Leadership is needed to be both socially accountable and technologically advanced and ethically aware. This chapter combines theoretical with practical's, painting information security and privacy picture and offers help to academics, policymakers, practitioners, and students hoping to penetrate and deal with challenging data security and privacy circumstances. Instead of proposing specific and seductive solutions, it attempts to offer readers the analytic resources that allow them to wander through the digital labyrinth by means of intelligent resilience and moral posture.

Quantifying Factors Influencing the Adoption of Internet Banking Services in Greece
M. Makris, V. Koumaras, H. Koumaras, A. Konstantopoulouand S. Konidis (2009). *International Journal of E-Adoption (pp. 20-32).*
www.irma-international.org/article/quantifying-factors-influencing-adoption-internet/1828