


Chapter 6

Sovereignty Over Personal Data: Legal Frameworks and the Quest for Privacy in the Digital Age

Andreja Primec

 <https://orcid.org/0000-0002-5615-7299>

University of Maribor, Slovenia

Gal Pastirk

 <https://orcid.org/0009-0001-7877-639X>

University of Maribor, Slovenia

Igor Perko

 <https://orcid.org/0000-0002-6101-1091>

University of Maribor, Slovenia

ABSTRACT

The contribution focuses on an individual's right to control their personal data and the right to privacy, emphasizing the legal aspects and developments in the context of modern technological and digital challenges. These rights become especially critical in the context of swift advancements in technology and digitalization, enabling the accumulation, examination, distribution, and sharing of extensive data volumes in previously unattainable manners. There has been a surge in sensors embedded within smart devices, gathering data from various aspects of our professional and personal lives. Furthermore, artificial intelligence (AI) has emerged, capable of analysing and interpreting data in unthinkable ways. These shifting dynamics present a challenge to reconsider how data is regulated. It's not merely about updating the rules themselves; it involves reimagining the process of creating regulatory frameworks.

DOI: 10.4018/979-8-3693-3334-1.ch006

INTRODUCTION

Artificial intelligence overwhelms us in our private and business lives at every turn. The data that fuels its operation and further development is becoming increasingly valuable. Big companies managing vast amounts of data are therefore more successful in developing new tools and devices, making their products more efficient and reliable. In this battle for data, private companies, which started to acquire data with the advent of the Internet and have since seen their collections “skyrocket”, are generally the winners. Personal data, which in its most general sense means “any information relating to an identified or identifiable individual” (Article 4(1) of the GDPR), occupies an essential place in private databases. Understanding and protecting this data is becoming increasingly important in the digital age, where privacy and personal data protection remain at the forefront of ethical and legal debates.

The right of individuals to control their data is a fundamental concept in modern data protection and privacy. This right is recognised and guaranteed in many international and national legal frameworks. One of the most well-known and influential examples is the European Union's General Data Protection Regulation (GDPR), cited above, which came into force in May 2018. The GDPR has set new privacy and data protection standards for individuals within the European Union (EU) and the European Economic Area (EEA). It sets out the rights of individuals about their personal data and the obligations of organisations that process that data. Of particular note is its extraterritorial reach, as it also applies to controllers or processors outside the EU who process individuals' data in the EU or monitor their behaviour within the EU (Ryngaert & Taylor, 2020). This means that the provisions of the GDPR must be respected by any company that processes European citizens' data (Martins Gonçalves, Mira da Silva & Rupino da Cunha, 2023) to strengthen the protection of fundamental rights and create fair competition in the EU market (Gömann, 2017).

The GDPR is considered the most modern data protection legislation in the world. The California Consumer Privacy Act of 2018 (CCPA) in the US (State of California, Department of Justice, 2018), the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada (Government of Canada, 2019) and the Lei Geral de Proteção de Dados Pessoais (LGPD) in Brazil (Presidência da República, Secretaria-Geral Subchefia para Assuntos Jurídicos, 2018), which, like the GDPR, lay down rules for the protection of citizens' privacy and personal data, and the obligations of companies that process the data, also play an essential role. However, there are also differences between them. In the EU and Canada, there is centralised control over the use of personal data in the private sector. At the same time, the US has minimal regulation, focusing on protecting freedom from government intrusion (Levin & Nicholson, 2023). As the authors of this paper are from

29 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/sovereignty-over-personal-data/352994

Related Content

Democratizing Information: Public Access as a Pillar of Governance

Nodir Jumaev, Anorgul Atajanova, Ogabek Solayevand Munir Ahmad (2026). *Legal and Regulatory Perspectives on Electronic Records as Evidence* (pp. 1-32).

www.irma-international.org/chapter/democratizing-information/398256

User Design: A Case Study in Developing Workplace Curricula

Robert Anthony Jordanand Alison Carr-Chellman (2017). *Medical Education and Ethics: Concepts, Methodologies, Tools, and Applications* (pp. 829-846).

www.irma-international.org/chapter/user-design/167320

Cross-Country and Cross-Sector CSR Variations: A Comparative Analysis of CSR Reporting in the U.S., South Korea, and Turkey

Altay Dikeç, Victor Kaneand Nejat Çapar (2017). *Comparative Perspectives on Global Corporate Social Responsibility* (pp. 69-95).

www.irma-international.org/chapter/cross-country-and-cross-sector-csr-variations/162806

Financial Sector Reforms in South Asian Countries

Amir Manzoor (2016). *Financial Market Regulations and Legal Challenges in South Asia* (pp. 36-50).

www.irma-international.org/chapter/financial-sector-reforms-in-south-asian-countries/147797

The Ethical Dilemmas of ChatGPT: Balancing Innovation and Responsibility

Bhavna Taneja, Pooja Shuklaand Aanya Taneja (2026). *Navigating the Risks and Rewards of ChatGPT: Governance, Innovation, and Ethical Challenges* (pp. 195-224).

www.irma-international.org/chapter/the-ethical-dilemmas-of-chatgpt/390728