Chapter 9
Cybersecurity, Data Protection, and Ethics in Digital Government:
Emotional Stability and Institutional Trust in the Age of Artificial Intelligence

Miguel Ruiz Jaimes
https://orcid.org/0000-0002-2585-9896
Universidad Politécnica del Estado de Morelos, Mexico

Yadira Toledo Navarro
Universidad Politécnica del Estado de Morelos, Mexico

Marco Antonio García Márquez
https://orcid.org/0000-0002-0644-4839
Universidad Politécnica de Pachuca, Mexico

José Efrén Marmolejo Valle
https://orcid.org/0000-0002-7191-4489
Universidad Autónoma de Guerrero, Mexico

Manuel Erazo Valadez
https://orcid.org/0009-0005-2530-8532
El Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET), Mexico

Angel Israel Daza-Castillo
El Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET), Mexico

Tlaloc Humberto Vergara Morales
https://orcid.org/0009-0008-3823-5784
El Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET), Mexico

ABSTRACT

This chapter explores the intersection of cybersecurity, data protection, and digital ethics in government, emphasizing how secure and transparent digital environments

DOI: 10.4018/979-8-3373-5535-1.ch009

influence citizen trust and emotional well-being. Building on the conceptual model of synthetic happiness, it argues that digital security is not only a technical requirement but a foundation for institutional legitimacy in AI-driven societies. The discussion incorporates international legal frameworks such as GDPR, NIST CSF, and ISO 27001, along with national laws like Mexico's LGPDPPSO, to illustrate challenges in harmonizing cross-border data policies. It also analyzes ethical considerations surrounding algorithmic bias, AI transparency, and surveillance, presenting best practices including explainable AI, blockchain-based accountability, and citizen participation platforms. Through a multidisciplinary approach, the chapter proposes strategic recommendations for governments to build inclusive, ethical, and emotionally resilient digital ecosystems.

1. INTRODUCTION

In a society that is becoming more reliant on automated systems and digital platforms, cybersecurity is no longer just a technical issue it's a key part of emotional well-being and social stability. Ruiz-Vanoye et al. (2025) introduced the idea of Synthetic Happiness, organized through a hierarchical pyramid. The first level Digital Security and Stability forms the foundation of the emotional ecosystem. This level includes data privacy, strong encryption, protection against cyberattacks, and reliable digital environments. These factors allow citizens to use public services, healthcare, and education managed by AI without fear or uncertainty.

Government digitalization has brought many benefits, such as better efficiency, automation, and easier access to services. However, it has also created new opportunities for attacks: identity theft, ransomware targeting public platforms, and manipulation of election data are just a few threats that directly affect the digital citizen's sense of security. The model proposed by Ruiz-Vanoye et al. (2025) suggests that if the first level security fails, the higher levels of emotional well-being will collapse. That's why government strategies should be based on the principle of "security by design. "

The use of artificial intelligence in government processes raises ethical questions about data use, automated decision-making, and algorithmic discrimination. Ruiz-Vanoye et al. (2025) emphasize that emotional wellbeing depends not just on technology, but on how it is managed. Ethics in AI such as algorithm transparency, decision traceability, and protection against bias becomes a key factor that strengthens the credibility of institutions and the sense of fairness felt by citizens.

Based on the work of Ruiz-Vanoye et al. (2025), who believe cybersecurity is a key part of how emotions influence societies that depend a lot on AI, new global research backs up this idea. Silva et al. (2024) studied more than 3,000 public digital