Chapter 6
Enhancing Cybersecurity, Privacy Innovation, and E-Government Readiness in Smart Cities:
A Framework for Awareness and Resilience

Mohammed Hussain Alsaad
https://orcid.org/0009-0002-9384-7819
Management and Science University, Malaysia

Muhammad Irsyad Abdullah
https://orcid.org/0000-0002-7840-2662
Management and Science University, Malaysia

Balqees Yaseen Alhaddad
Universiti Geomatika Malaysia, Malaysia

ABSTRACT

The increasing dependence of urban societies on digital infrastructure has brought with it a wide range of cybersecurity and privacy challenges. These issues are no longer limited to technical systems alone—they are now deeply tied to how people understand, trust, and interact with digital services, especially when those services come from public institutions. This chapter looks at these challenges from a broader perspective. It proposes a flexible framework that's not only built with the help of AI tools, but also rooted in real-life concerns faced by communities. The model emphasizes raising awareness, protecting user data, and building confidence in how

DOI: 10.4018/979-8-3373-4455-3.ch006

digital governance is practiced. By paying attention to cultural differences and the actual experiences of people using these systems, the chapter presents strategies that can help cities become more transparent, resilient, and better prepared for future digital risks.

1. INTRODUCTION: SETTING THE STAGE FOR SMART CITIES IN A DIGITAL AGE

The digitalization of cities has been driving the development of the 'smart city', a paradigm of urban design that comprises the implementation of internet-connected infrastructure, analytics on real time data and devices inter-connectivity for optimizing the effectiveness, sustainability and efficient delivery of civic services (Almeida, 2023; Khan et al., 2022). Innovations like smart traffic management to AI driven waste collection have changed the way cities function as well as how inhabitants engage with public spaces. Yet with the potential of smart cities comes cybersecurity, privacy and equity issues. The pace of digital evolution has overtaken the associated governance, and many cities are ill-equipped to deal with the ethical, legal and social aspects of data driven urbanism (Bannerman & Orasch, 2020; Mohamed et al., 2020). This disconnects between technological innovation and institutional readiness highlights the need for frameworks that facilitate digital transformation while protecting rights, building trust and ensuring it's inclusive. The deployment of smart technologies in cities creates a complex risk landscape, including technical vulnerabilities in Internet-of-Things (IoT) devices and algorithmic biases that reinforce inequalities faced by certain groups (Ismagilova et al., 2022; Ayalon & Toch, 2021). In addition, the accumulation and exploitation of huge amounts of personal and behavioral data defy traditional understandings of privacy and responsibility, particularly in countries with modest or inconsistent legal protections (Rizi & Seno, 2022; Artyushina, 2023). Just as urgent is the problem of digital inequality. A digital divide between the digitally fluent and those caught out by innovation, lacking infrastructure or access to these tools, is being exacerbated. In that sense, e-government readiness defined as the institutional and infrastructural capacity to provide public services through digital means is a necessary requirement for smart city success (Kuzior et al., 2023; Hossain et al., 2024). Such projects, smart city included, may inadvertently cement structural inequalities and increase civic disengagement if the design isn't proactively considerate and inclusive.

With this context in mind, this chapter suggests a Four-Pillar framework for promoting resilient and human rights-based smart city governance. Building on interdisciplinary literature, global case applications, and emerging policy initiatives, our framework highlights: (1) secure and interoperable infrastructures; (2) embed-