Chapter 2
Cybersecurity and Human Rights in South Asia:
A Legal and Governance Perspective Through Case Studies

Abhilash Aggarwal
https://orcid.org/0009-0000-2146-1170
Rai University, India

ABSTRACT

South Asia, encompassing countries like India, Sri Lanka, and Bangladesh, has witnessed rapid digital growth, driven by high mobile penetration and the adoption of digital financial services. As of December 2024, India alone had 970 million internet subscribers, with a 54% annual data consumption growth rate, while Bangladesh reported 50% household internet penetration. However, this digital transformation has been accompanied by a surge in cyberattacks, posing significant challenges to governance, human rights, and privacy. This chapter examines three major cyberattacks in South Asia, the 2022 AIIMS ransomware attack in India, the 2023 Sri Lankan government cloud system attack and the 2016 Bangladesh Bank heist, through a legal and governance lens, analyzing their implications

DOI: 10.4018/979-8-3373-5992-2.ch002

for human rights and privacy. By providing descriptive and historical analyses, the chapter aims to contribute to the discourse on cybersecurity, ethical considerations and human rights in the region.

INTRODUCTION

South Asia's digital landscape has undergone explosive growth, transforming economies and societies through widespread internet adoption and mobile connectivity. The region's cybersecurity landscape is shaped by its unique socio-political and economic context. Rapid digital adoption, coupled with uneven cybersecurity investments, has made South Asia a prime target for cybercriminals (Gamboa, 2025). The evolution of cyber threats over the past two decades mirrors the rapid expansion of digital infrastructure, shifting from rudimentary, often ideologically driven attacks to highly sophisticated, profit-oriented operations that pose profound risks to economies, governance and human rights (Malik et al., 2025). For example, India faced 375 cyberattacks daily in 2020, with a 261% increase in Q1 2024 (PTI, 2020; The Cyber Express, 2024). Legal frameworks, such as India's Information Technology Act, 2000 (IT Act) and Bangladesh's National ICT Strategy, have struggled to keep pace with these threats, often lacking robust mechanisms to protect human rights in the digital realm.

Cybersecurity Definitions in Global and Regional Treaties and Conventions

Cybersecurity, while not always explicitly defined in international treaties and conventions, is commonly addressed through related concepts like information security, network protection, and defences against cyber threats. In global instruments, definitions often focus on foundational elements to facilitate cooperation on cybercrime rather than providing a standalone definition of cybersecurity. For instance, the *Budapest Convention on Cybercrime* of 2001, adopted by the *Council of Europe* and acceded to by many countries worldwide, does not explicitly define cybersecurity but implies it through a framework for criminalizing and cooperating