Chapter 8
The Impact of Cybersecurity Laws on the Child Safety in the Digital World

Sarita Kadian
https://orcid.org/0000-0002-5017-2543
Bharati College, University of Delhi, India

Nikita Yadav
Bhagini Nivedita College, University of Delhi, India

Garima Yadav
Algoma University, Brampton, Canada

ABSTRACT

In today's digital era, children benefit from vast online opportunities but also face threats like cyberbullying, grooming, sextortion, and identity theft. India's legal safeguards—such as the IT Act, POCSO Act, and IPC provisions—address these risks, yet enforcement gaps, outdated laws, and limited cybercrime expertise undermine their effectiveness. As threats evolve with AI and IoT technologies, India must modernize its legal framework, drawing from global models like the GDPR, OECD guidelines, and the UK's Age-Appropriate Design Code. A multi-stakeholder approach involving policymakers, educators, tech companies, and parents is essential. Key steps include enhancing digital literacy, mandating safety-by-design practices, and strengthening data protection laws. With coordinated efforts, India can create a secure digital ecosystem where children are empowered to explore safely.

DOI: 10.4018/979-8-3373-5132-2.ch008

INTRODUCTION

Digital technology has reshaped childhood, offering vast opportunities for learning and connection—but also exposing children to serious online risks like cyberbullying, grooming, and privacy violations. As digital natives, many children lack the maturity to navigate these dangers, making them particularly vulnerable. This highlights the importance of cybersecurity as more than a technical measure—it is a vital, multi-layered system involving legal, educational, and policy-based protections. Laws must regulate harmful content, enforce age-appropriate access, and punish online crimes targeting children. To protect children's safety and rights, cybersecurity frameworks must remain adaptive, inclusive, and responsive to the evolving digital landscape.

Overview of Cybersecurity and Child Safety

In an increasingly interconnected world, digital platforms have become an integral part of children's lives. From accessing educational resources to social networking and entertainment, the internet offers boundless opportunities. However, with these opportunities come unprecedented threats. Cybersecurity concerns, once predominantly limited to the financial or corporate realm, now deeply intersect with child welfare. As children spend more time online, their exposure to cyberbullying, exploitation, and privacy violations intensifies. Cybersecurity in the context of child safety refers to the frameworks, technologies, and laws designed to safeguard minors from harm in digital environments. This is illustrated in Figure 1, which outlines the core pillars of cybersecurity laws—ranging from data protection and online privacy to content regulation and age restriction—essential for ensuring child safety in the digital world.

Children, unlike adults, often lack the cognitive maturity to fully grasp the implications of their online actions. Their vulnerability is exacerbated by a lack of digital literacy and the rapidly evolving nature of cyber threats. A child might unknowingly share sensitive information or engage with malicious content. Consequently, the role of cybersecurity extends beyond technical protection—it encompasses education, awareness, and the cultivation of a safe digital culture that prioritizes children's rights.