Chapter 10
Cybersecurity Laws and Child Protection: Strengthening Digital Safety Frameworks

Andi Asrifan
https://orcid.org/0000-0002-9934-6129
Universitas Negeri Makassar, Indonesia

ABSTRACT

Cybersafety for children is a global priority as they use technology more. Cybersecurity regulations and child protection are changing, and this chapter discusses digital safety concerns and solutions. It emphasizes legislative reforms, digital literacy, and responsible technology development to address increasing cyber hazards such as online exploitation, cyberbullying, identity theft, and AI-driven risks. The chapter also examines parents, educators, and technology corporations' roles in digital security. To reduce hazards and improve online child safety, it emphasizes international cooperation and ethical AI deployment. By adopting comprehensive regulations, proactive education, and improved cybersecurity solutions, stakeholders may establish a safer digital ecosystem for future generations, allowing children to benefit from digital breakthroughs while remaining cyber-safe.

DOI: 10.4018/979-8-3373-5132-2.ch010

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

INTRODUCTION TO CYBERSECURITY AND CHILD PROTECTION

Understanding Cybersecurity in the Digital Age

Digital technology have transformed communication, education, and entertainment in the 21st century (Ong & Annamalai, 2024; Singh, 2021). The internet is essential for worldwide communication, infinite information, and virtual experiences. Despite these benefits, cybersecurity threats have skyrocketed, heightening online safety worries, especially for children. Cybersecurity encompasses procedures, technology, and policies that safeguard networks, devices, and data from unauthorized access, cyberattacks, and exploitation.

Smartphones, social media, and AI have transformed the digital world (Kumar et al., 2024; Tran, 2025). These advances provide convenience, learning, and social engagement, but also enormous risks. Digital natives grow up with internet interactions. However, their lack of understanding and digital literacy puts children vulnerable to cyberbullying, online grooming, identity theft, and improper content. Without strong cybersecurity, children's online safety is at stake.

Governments, organizations, and tech firms realize these issues' urgency. Cybersecurity laws and regulations reduce hazards, ensure digital safety, and encourage responsible online activity. However, many legislative frameworks struggle to keep up with rapid technology improvements, leaving child protection loopholes. Cybersecurity measures must adapt to new threats and protect youngsters online (Li, 2024).

Cybersecurity is a social, ethical, and technological issue. To make the internet safer, governments, educators, parents, and technology companies must work together. Digital literacy, parental controls, and ethical AI development are essential for children's online safety (Banić & Orehovački, 2024; Berson et al., 2024). To teach kids how to use the internet responsibly, schools must teach cybersecurity.

Building complete kid protection procedures starts with understanding cybersecurity in the digital age. Rapid technological growth requires proactive steps to protect young users from online risks, allowing them to benefit from digital advancements without risking their safety and well-being (Jang & Ko, 2023; Paat & Markham, 2021). This chapter lays the groundwork for cybersecurity regulations and digital safety policies to protect children in the ever-changing cyber ecosystem.

The Growing Risks to Children Online

As digital technology grows more integrated into daily life, children face online hazards that jeopardize their safety, privacy, and well-being (Perez et al., 2021; Ognibene et al., 2023). The internet has many educational and social benefits, but

32 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/cybersecurity-laws-and-child-protection/386102

Related Content

A New Framework for Matching Forensic Composite Sketches With Digital Images

Chethana H. T.and Trisiladevi C. Nagavi (2021). *International Journal of Digital Crime and Forensics (pp. 1-19).*

www.irma-international.org/article/a-new-framework-for-matching-forensic-composite-sketches-with-digital-images/283124

On More Paradigms of Steganalysis

Xianfeng Zhao, Jie Zhuand Haibo Yu (2016). *International Journal of Digital Crime and Forensics (pp. 1-15).*

www.irma-international.org/article/on-more-paradigms-of-steganalysis/150855

Distributed Privacy Preserving Clustering via Homomorphic Secret Sharing and Its Application to (Vertically) Partitioned Spatio-Temporal Data

Can Brochmann Yildizli, Thomas Pedersen, Yucel Saygin, Erkay Savasand Albert Levi (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 395-415).*

www.irma-international.org/chapter/distributed-privacy-preserving-clustering-via/60961

A Forensic Tool for Investigating Image Forgeries

Marco Fontani, Tiziano Bianchi, Alessia De Rosa, Alessandro Pivaand Mauro Barni (2013). *International Journal of Digital Crime and Forensics (pp. 15-33).*

www.irma-international.org/article/a-forensic-tool-for-investigating-image-forgeries/103935

Source Camera Identification Issues: Forensic Features Selection and Robustness

Yongjian Hu, Chang-Tsun Li, Changhui Zhouand Xufeng Lin (2011). *International Journal of Digital Crime and Forensics (pp. 1-15).*

www.irma-international.org/article/source-camera-identification-issues/62074