Chapter 9
Cyber Laws and their Role in Safeguarding Children Online

Yagyanath Rimal
https://orcid.org/0000-0003-1045-7728
Pokhara University, Nepal

Hitesh Rawat
https://orcid.org/0009-0006-7171-6016
University of Extremadura, Spain

Antonio González-Torres
Costa Rica Institute of Technology, Costa Rica

Sanjaya Kumar Sarangi
Utkal University, Bhubaneswar, India

Anjali Rawat
https://orcid.org/0009-0006-7171-6016
University of Extremadura, Spain

ABSTRACT

This study evaluates the effectiveness of Nepal's cyber laws in safeguarding children from online threats by analyzing legal frameworks, digital safety awareness, and enforcement practices. Utilizing data from the 2024 Nepal Cyber Awareness Survey (NCAS-2024), which gathered 3,500 responses from students, parents, teachers, and law enforcement across all provinces, it adopts a mixed-method approach. Legal analysis is integrated with the Regulatory Impact Assessment Model (RIAM) to assess performance using metrics like reporting rates, response times, and digital

DOI: 10.4018/979-8-3373-5132-2.ch009

literacy. Results indicate that only 41.2% of respondents are aware of child protection provisions in the Electronic Transactions Act (ETA) 2063, and just 28.7% of cyber incidents involving minors receive prompt legal action. In contrast, areas with active digital literacy programs report a 55.4% reduction in cyber threats to children. The study underscores the need for improved enforcement, legislative updates, and greater public awareness to enhance child online safety in Nepal.

INTRODUCTION

With the rapid expansion of internet accessibility in Nepal—where over 11.51 million people (approximately 38% of the population) are active internet users as of 2024—the online safety of children has become a critical concern. The rise of social media (Bhardwaj et al., 2024) (Dhawan et al.,2025), mobile applications, and online learning platforms has exposed children to various cyber risks, including cyberbullying (Mascari et al.,2025) (Nahar et al.,2023), online grooming, sexual exploitation, and privacy breaches (Pithawa et al., 2023). Although Nepal introduced the Electronic Transactions Act (ETA) 2063 and later expanded its provisions through the Cyber Security Policy 2023, enforcement and child-focused digital protections remain inconsistent and under-resourced.

To evaluate the efficacy of these laws, this research employs a hybrid legal-tech approach using Natural Language Processing (NLP) for legal document analysis and Sentiment Analysis powered by BERT-based models to assess public perception from social media posts and online forums. Additionally, the study integrates Case-Based Reasoning (CBR) and Comparative Statutory Analysis (CSA) to compare Nepal's cyber legislation with international frameworks such as the EU's General Data Protection Regulation (GDPR) and India's IT Act (Amendment 2021). Data is drawn from the Nepal Cyber Awareness Survey Dataset 2024 (NCAS-2024) (Atkinson-Sheppard et al., 2025) (Adhikari et al., 2025) (Tariq et al., 2025) and a curated set of 58 child-related cybercrime cases recorded by the Nepal Police Cyber Bureau (Rijal et al., 2025) (Budhathoki, 2025) (Bhandari, 2025) (Dahal, 2025) (Adhikari et al., 2025) (Cole and Kim,2025) (Acharya et al., 2025) between 2020 and 2023. Among these cases, 67% involved social media exploitation, and 19% were linked to online gaming and anonymous chat platforms. Despite the existence of legal provisions, only 34% of the cases resulted in successful prosecution, primarily due to digital evidence handling challenges and lack of specialized investigative resources.

By using a Regulatory Impact Assessment Model (RIAM) and visualized analytics through tools like Tableau and Power BI, the study highlights both the strengths and limitations of Nepal's current cyber legal structure in protecting minors online. This interdisciplinary methodology enables a data-driven critique and proposes actionable