Chapter 6
The Impact of Cybersecurity Laws on Child Safety in the Digital World:
A Global Perspective

Antonio Gonzalez-Torres
https://orcid.org/0000-0001-5427-0637
Costa Rica Institute of Technology, Costa Rica

ABSTRACT

This study investigates the role of cybersecurity legislation in protecting minors from cyber threats by analyzing its influence on the frequency of child-targeted digital crimes. Drawing on diverse sources—including the Global Child Online Safety Index (G-COSI 2023), Interpol Cybercrime Reports (2023), and the UNICEF Online Child Protection Survey (2022–2023)—a hybrid methodology was employed, integrating Random Forest classification with Latent Dirichlet Allocation (LDA) for legal text analysis and threat prediction. Results show that nations with well-established cybersecurity frameworks experience 42% fewer cases of online child exploitation and 37% fewer phishing attempts against minors. The Random Forest model demonstrated strong performance (accuracy: 89.6%, precision: 85.2%, recall: 88.3%). Topic modeling revealed that provisions on data privacy, digital education, and mandatory reporting are key legal factors reducing harm. The findings emphasize the vital impact of cohesive cybersecurity policies in creating safer digital environments for children.

DOI: 10.4018/979-8-3373-5132-2.ch006

INTRODUCTION

In an era where digital interaction (Rawat et al., 2025) is an integral part of childhood, ensuring the safety of minors online has become a global priority. The proliferation of social media, gaming platforms, and online learning (Rajavat et al., 2024) environments has exposed children to a spectrum of cyber threats, including grooming, phishing, cyberbullying, and data exploitation. According to UNICEF (2023), over 1.2 billion children globally are active internet users, with 64% engaging on social media platforms before the age of 13, often bypassing age verification protocols.

Recent cybercrime (Rawat and Rajavat,2024a) investigations, such as Interpol's Operation HAECHI-IV (2023), revealed a 39% rise in child-targeted phishing schemes and online abuse cases compared to 2022. In response to such alarming trends, governments have enacted cybersecurity laws to establish regulatory protections, enhance digital literacy (Mishra et al., 2024), and enforce platform accountability. For instance, the EU's Digital Services Act (2023) mandates proactive content moderation, while the U.S. Kids Online Safety Act (KOSA) focuses on mental health and privacy protections for users under 18.

To measure the effectiveness of these laws, this study integrates Natural Language Processing (NLP) (Bhardwaj et al., 2024) (Dhawan et al., 2025) (Mascari et al.,2025) for legislative text analysis and Random Forest classifiers for predicting child safety outcomes based on cyber incident reports. Additionally, Graph Neural Networks (GNNs) are employed to model and visualize relationships between legal measures and threat vectors across nations. Data sources include the Global Child Online Safety Index (2023), Cybersecurity & Infrastructure Security Agency (CISA) threat (Rawat and Rajavat,2024b) database, and UNICEF's Online Risk Behavior Survey covering over 80 countries.

Preliminary analysis shows that countries with child-focused cybersecurity policies experience 45% fewer cyberbullying incidents and 51% lower exposure to explicit content among minors. These figures underscore the tangible impact of well-structured legal frameworks in reducing digital risks for children (Chirgaiya and Rajavat,2023). This study not only evaluates the global landscape of child-centric cybersecurity (Nahar et al.,2023) (Pithawa et al., 2023) laws but also introduces a data-driven framework for identifying policy gaps and predicting areas of vulnerability, thus supporting evidence-based policy reform.