Chapter 12
Digital Literacy Initiatives, Policy Evaluation, and Machine Learning:
Cyber Laws and Their Role in Safeguarding Children Online

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

Prathamesh Muzumdar
https://orcid.org/0000-0002-9000-363X
Mangalayatan University, India

Priya Matta
Tula's Institute, Dehradun, India

A. Samson Arun Raj
https://orcid.org/0000-0001-5090-5199
Karunya Institute of Technology and Sciences, India

Kuldeep Singh
https://orcid.org/0000-0003-1011-6085
Arkansas Tech University, USA

Sanjaya Kumar Sarangi
Utkal University, Bhubaneswar, India

ABSTRACT

As digital education and social media grow rapidly in India, children face increasing risks online, including cyberbullying, exploitation, and exposure to harmful content. This study assesses how effectively Indian cyber laws protect minors in the digital space. A new approach—Legal-Empirical Safeguard Analysis Method (LESAM)—was used, combining legal analysis with real-world data. The study analyzed 7,842 child-targeted cybercrime cases reported to the NCRB from 2018 to 2023. LESAM utilized policy evaluation and machine learning (Random Forest) to classify incidents by severity and response. Findings revealed that 63.4% of cases were handled under the IT Act (2000), while 21.8% involved the POCSO Act. The

DOI: 10.4018/979-8-3373-5132-2.ch012

model accurately identified high-risk cases 91.7% of the time. While current laws provide a strong foundation, enforcement gaps and limited public awareness persist. The study calls for better digital literacy initiatives and improved inter-agency coordination to enhance child safety online.

INTRODUCTION

The rapid expansion of the internet has brought significant opportunities for children to access information, interact socially, and engage in learning. However, this increased digital presence has also exposed minors to a rising tide of online threats (Rawat et al., 2025) (Rajavat et al., 2024), including cyberbullying (Bhardwaj et al., 2024) (Dhawan et al.,2025), online grooming, and exploitation. In response, countries across the globe, including India, have implemented various cyber laws to safeguard children from these dangers. Despite the existence of legal frameworks, such as the Information Technology Act (2000) and the Protection of Children from Sexual Offences (POCSO) Act (2012), the enforcement and effectiveness of these laws remain a topic of concern.

Types of Parental Control Techniques

Parental control techniques are strategies and tools used by guardians to monitor, manage, and influence the digital behavior of children. With the widespread use of smartphones, tablets, and computers among minors, these controls have become crucial. A 2023 report by Statista revealed that around 72% of parents in the United States use some form of parental control to manage their children's online activity. Below are the primary types of parental control techniques:

Content Filtering

Content filtering (Mascari et al., 2025; Nahar et al., 2023) is one of the most widely used methods. It blocks access to inappropriate or harmful websites, videos, and applications. For example, tools like Net Nanny and Kaspersky Safe Kids allow parents to block content categories such as gambling, adult content, and violence.

- Usage Rate: According to a Pew Research study (2023), 58% of parents use content filters to protect their children.
- Effectiveness: Studies show content filtering can reduce exposure to inappropriate material by around 67%.