

# IARCO\_FinalDraft - Odrita Ahmed.pdf

*by Sanaul Haque*

---

**Submission date:** 13-Oct-2025 10:51PM (UTC+0700)

**Submission ID:** 2779950057

**File name:** IARCO\_FinalDraft\_-\_Odrita\_Ahmed.pdf (177.21K)

**Word count:** 2907

**Character count:** 16512

**IARO Research Proposal**

Odrita Ahmed

Sunnydale School

Junior

AS Level

Bangladesh

September 30, 2025

[odrita.ahmed123@gmail.com](mailto:odrita.ahmed123@gmail.com)

**Research Topic:** Assessing how Bangladesh can design robust, child-centred cybersecurity laws for minors that effectively prevent and mitigate online harm while respecting children's rights and autonomy.

## **Assessing how Bangladesh can design robust, child-centred cybersecurity laws for minors that effectively prevent and mitigate online harm while respecting children's rights and autonomy**

### **Research Problem**

Recently, internet usage among children in Bangladesh has grown very rapidly, but unfortunately, this growth has outpaced the legal and protective systems designed to keep these children safe. Reports show that a growing number of Bangladeshi teenagers and younger children are using the internet regularly; they are mainly using social media, private messaging apps, and participating in online gaming, often without adult supervision. At the same time, adolescents are being increasingly exposed to the harms of cybercrimes, with cases of online grooming and extortion, cyberbullying, rampant access to harmful content and all sorts of other harassment among minors reaching an all-time high.

Given that Bangladesh is going through a rapid digital reformation, in addition to facing rising reports of cybercrime being perpetrated against minors. It is necessary to design a comprehensive and unambiguous, child safety-focused cybersecurity protection policy for Bangladeshi youth. In practice, these laws should not only safeguard children's rights but also respect their autonomy. Simultaneously, they need to be able to fit within Bangladesh's existing legal system in a way that is both realistic and enforceable. Alongside these, the need for preventive measures which allow minors to safely navigate through the digital landscape has also become increasingly prevalent.

Despite general cybersecurity laws and child protection laws already existing, these policies often lack specialised guidelines for minors. Vague definitions of crimes, legal protection regarding children being limited, weak enforcement, especially in Bangladesh, and limited awareness of these laws make them less effective. These issues allow online criminals to exploit legal gaps. Taking advantage of limitations while victims, specifically children, struggle to adequately protect themselves. Additionally, these laws usually do not offer any preventive measures, such as preventing the interaction of adults and minors online through age verification.

These laws often do not meaningfully take into account present vulnerabilities. However, in the current digital environment, children face huge developmental risks from being victims of these cybercrimes, for example, depression, anxiety and other long-term neurological disorders. Moreover, future proposed legislations fail to take into account these pitfalls. Transparency International argues that the proposed Cyber Security Rules 2024 lack child-focused protections and clarity. Offering unclear definitions and a lack of comprehensiveness[1].

Therefore, this project proposes to design a child-centred cybersecurity legal framework, directly incorporating empirical evidence from adolescent cybercrime victims and stakeholder input, to create adequate protective safeguards for Bangladeshi minors. This study would also attempt to implement precautionary measures to inhibit the increase in the rate of cybercrimes against minors by researching the effectiveness of such preventative measures.

### **Existing Literature**

These studies establish both the prevalence of online harm and its psychological risks. This literature finds serious harm caused by online crime, legal shortcomings of current policies, and the need for a more concise, child-rights-centred approach. Yet these reports lack a legal design study and research on preventative measures, specifically on what a child-centred cybersecurity law should look like in Bangladesh. While gaps in legislation are found or highlighted in numerous papers and reports, the research, however, fails to find other avenues of protection through empirical data. Such as what this legislation should look like, specifically for holding criminals accountable while protecting victims, and for defending the online digital rights of minors, even when protecting them from cybercrimes

#### **Empirical Reports**

**Mubassara et al. [2]** *Cyber Child Abuse in Bangladesh: A Rural Population-Based Study* found that more than half of surveyed rural children reported experiencing at least one type of online abuse, ranging from bullying to exposure to unsolicited explicit content. This article shows the concerning rise in cybercrime in Bangladesh. **Noor et al. [3]** reported a strong association between cyberbullying and the incidence of depressive disorders among female adolescents in Bangladesh. This study shows a direct relation between online harassment and long-lasting mental health issues in young children. This proves the necessity of protecting children from cyberbullying.

**Islam et al. [4]** This qualitative study in Bangladesh explores the root causes of online child sexual abuse (OCSA). It finds that low digital literacy, unsafe online habits and systematic inadequacies are some reasons behind this problem. The study recommends integrating OCSA education in schools, implementing anonymous reporting systems, and strengthening legal measures. This study proves that there are current limitations in the legal framework concerning this topic. It showcases the legislative failings of outdated policies that are one of the main causes of OCSA.

**Towhid et al. [5]** *Protecting children from online sexual abuse in Bangladesh: A policy brief* showcases policy implications of these harms. This policy brief reviews the growing challenge of online sexual abuse of children in Bangladesh and highlights systemic gaps

in the statutes meant to protect them. The authors highlight an urgent demand for policies tailored to children's online safety and emphasise the importance of integrating digital literacy education, along with clearer and less equivocal policy measures. The policy brief calls attention to the dire state of the current policies, which are insufficient in protecting minors. However, while they do urge for stronger enforcement of the law and greater criminalisation of certain offences, they do not offer empirically grounded new legal statutes. These new frameworks are very important due to the rapidly changing digital landscape. The laws must develop as cyber criminals adapt to circumvent the current laws.

#### Policy Analyses

**Towhid.** [6]. In *Transparency Bangladesh - Cyber Security Rules Review*, it highlighted that the draft 2024 Cyber Security Rules lack clarity and sufficient child-focused safeguards. It also struggled to balance digital security with civil rights, demonstrating the need for balanced approaches that preserve digital autonomy. **Hossain et al.** [7]. This overview notes gaps in oversight and the inability of current policy to adapt to changing cyber threats, partially due to the lack of empirical data from actual cybercrime victims. This shows that the present statutes are not equipped to properly serve and protect adolescents online.

Despite this literature, key gaps remain, especially in stakeholder perspectives of actual children and their guardians, which are underexplored in Bangladesh. Legal design proposals that integrate empirical findings, such as actual risks and types of harm, with rights-protective drafting for minors, taking into account actual victims, are rare. Many studies focus on prevalence and correlation, but do not explore in depth how children or guardians can actually use the law.

Most reports call for the greater enforcement or criminalisation of cybercrime laws; however, they do not offer evidence-based legal solutions. As the future of the internet and, hence, cybercrime evolves, new policies must be created to overcome these crimes as they develop.. Legal analyses tend to critique what is there, rather than offering detailed alternative frameworks or drafting proposals with stakeholder input.

#### Research Question

How can Bangladesh design robust, child-centred cybersecurity laws that are empirically backed by the lived experiences of minors who have been victims of online crimes, to effectively prevent and mitigate cybercrimes while protecting children's rights and autonomy?

#### Methodology

In this study, a mixed-methods approach should be used, combining different forms of quantitative surveys, qualitative interviews, and a legal analysis. This methodology will be able to generate empirically grounded recommendations for child-centred cybersecurity law.

#### Quantitative Component

The quantitative strand will focus on the prevalence, severity and correlation of cyber victimisation among Bangladeshi minors. A sample of approximately 1,000 children aged 10-17 and 500 caregivers should be recruited using random sampling, so that a fair representation of minors in Bangladesh is surveyed. The study would attempt to include vulnerable minorities such as girls from lower-income households and out-of-school children in the program, as a large majority of victims tend to be less digitally literate [4].

This component will include a standardised questionnaire covering internet usage, exposure to various harms, i.e. cyberbullying, harassment, sexual solicitation, and privacy violations. Participants will undergo mental health screening through validated instruments such as the PHQ-9 for depression and the GAD-7 for anxiety. These questionnaires are very reputable and commonly used to screen adolescent mental health. Moreover, they are also short and simple enough for children to be able to comprehend and answer effectively. When conducting the surveys, limitations of the quality of research have to be taken into account, such as some children's inability to comprehend the questions or answer the questions truthfully.

Awareness of online rights and digital literacy should also be recorded using other simple questions. A 5-point Likert scale with 1 being Strongly Disagree and 5 being Strongly Agree, will be used throughout to measure responses effectively and to properly compare results. Some proposed sample questions are "I feel safe when using social media," and "Reporting online abuse leads to fair and helpful outcomes."

The overall style of the questions must be simple enough for a child to understand without assistance. Questions will need to be properly translated into Bengali as needed. A Likert scale is also very practical when dealing with children, as many young children may not have the capacity to write down an articulate response showing their actual thoughts.

Descriptive statistics may be used to sort cyber victimisation trends by demographics. Inferential statistics will be used to correlate cybercrimes to mental health among minors using regression analyses. Chi-squared tests and ANOVA can be used to compare exposure to online harm and the severity of the harm across different demographics.

#### **Qualitative Component**

For the qualitative aspect, in-depth personal interviews are required. 40–50 minors who have experienced cyber harms will be interviewed, alongside 15–20 caregivers and 15–20 other stakeholders such as teachers, police officers, and policymakers. These participants will take part in semi-structured interviews and subsequently focus group discussions.

An in-depth interview is the best way to qualitatively understand the participants' responses, as immediate clarification can be asked for, and the interviewee's response is not constrained or limited by format or the ambiguity of a typed response. The interviews will prioritise children's lived experiences. Nuance should be avoided for the minors' interviews. The questions must be comprehensible, and inadequate responses must be disregarded or clarified upon.

The interviews will attempt to bridge the gap between the failure of current policy to effectively protect minors and the minors' own experience with cybercrime and its related laws that may not have been visible in the quantitative survey. Sample questions may include "Do you feel that the current laws in place are adequate enough in protecting you against cybercrimes?". Questions may also include hypothetical scenarios.

In the interviews with other stakeholders, the topic of preventative measures, such as age restrictions on websites, age verification, and banning of minors in certain areas of the internet, should also be considered and expanded on, particularly in the Focus Group Discussion. Subsequently, minors' responses to such measures must also be recorded to calculate the effectiveness of these proactive measures, i.e. "How willing are you to lie about your age online?" or "Would banning minors from social media deter you from accessing such sites?"

Focus Groups should also be used. These focus groups with minors should be used to gather experiences with cybercrime, perceptions on how they believe the current laws work in protecting them, perceived barriers to reporting and seeking justice, etc. A focus group can bring about a greater insight into the issue at hand and how best to go about solving the problem at its root.

With this data, it is recommended that an analysis be performed to look for common themes, conflicting perceptions, and aspirational views of what protection laws should look like, which should then be used to create child-centric legislation. Afterwards, Thematic analysis can be used to simplify the data into understandable patterns that can be further analysed to create legal precedents.

#### **Policy Review Component**

When dealing with legislation, the study must also review Bangladesh's cyber laws, such as the Data Security Act 2018, the Cyber Security Act 2023 and the Proposed draft for 2024, to understand the limitations of these laws. A framework cannot be created without first examining the present policies and their constraints or hindrances. Limitations should also be extracted from the qualitative component, i.e. how caregiver and child protection officers believe the system has obstacles. These laws must then be compared with child protection laws in the UK, America, and the EU to find useful ideas that have been missed in Bangladeshi policies. These gaps are then used to suggest a child-focused cybersecurity law with clear rules and safeguards.

#### **Ethical Safeguard Considerations**

Before proceeding with the methodology, approval from the Institutional Review Board in Bangladesh and compliance with child-research guidelines are necessary. It is very important to ensure parental consent is recorded, as well as consent from the child. The study must be able to maintain confidentiality and anonymity. The researchers should avoid collecting identifying data unnecessarily, such as names or dates, especially on minors and instead use other anonymised identification methods for subjects, like numerical codes. It is also vital to train researchers and interviewers in trauma-informed interviewing. The child's safety must remain a priority, and any reports of abuse or harm must be reported to the responsible authorities.

#### **Research Importance and Conclusion**

This project is specified and critical. It proposes not only to document risks and their sources, but to design an actionable legal framework specifically for minors. By integrating quantitative data, qualitative lived experiences, and legal analysis, it can connect empirical research and policy design. As Bangladesh is in the process of revising its cybersecurity and digital safety framework, the need for more specified research is vital. Findings from this study could directly influence those reforms.

Bangladesh's development depends on equipping young people to use the internet confidently and safely, but current legal frameworks are not sufficient to ensure this, while also maintaining a nourishing online environment for Bangladeshi adolescents. This proposal is focused specifically on minors, a group often marginalised in research pertaining to cybersecurity laws, especially in the case of preserving civil rights in addition to protection, even though the future of digital development is dependent on the youth.

Cybercrime is constantly evolving to circumvent current laws, so creating new policies is imperative in combating these criminals. Moreover, the only way to effectively create safeguards for minors while also respecting autonomy is through research, and the only

way to accurately research to find limitations and possible avenues is by researching the lived experience of actual Bangladeshi cybercrime victims and other stakeholders.

This proposal is not only innovative but also essential because Bangladesh is at a digital inflection point. Child internet usage is rising, but the legal frameworks lag behind. As Bangladesh expands its digital infrastructure, the urgency of child-focused legislation becomes more pronounced. The result of this research proposal is not just academic but actionable; it provides a legal blueprint guided by empirical data.

#### Bibliography

- [1] Q. M. H. Supan, *Review of Proposed Cyber Security Rules, 2024*, Position Paper, Transparency International Bangladesh, pp 1-27, 13 June 2024, [Online]. Available: <https://www.ti-bangladesh.org/upload/files/position-paper/2024/pcsr/Review-of-proposed-Cyber-Security-Rules-2024-En.pdf>.
- [2] L. Mubassara, M. I. I. Towhid, S. Sultana, A. I. Anik, M. Salwa, M. M. H. Khan, and M. A. Haque, "Cyber Child Abuse in Bangladesh: A Rural Population-Based Study," *World Journal of Social Science*, vol. 8, no. 1, pp. 104–113, Jan. 2021, doi: 10.5430/wjss.v8n1p104.
- [3] S. T. A. Noor, M. F. Islam, M. S. Hossain, R. B. Islam, R. Banik, S. I. Shiblee, S. M. Nasrullah, and S. Raza, "The association of cyberbullying with major depressive disorders among Bangladeshi female adolescents: findings from the Bangladesh adolescent health and wellbeing survey 2019–20," *BMC Psychiatry*, vol. 25, no. 1, p. 783, Aug. 2025, doi: 10.1186/s12888-025-07234-z.
- [4] M. R. Islam, M. I. I. Towhid, M. Salwa, A. Tasnim, W. W. Mroy, M. M. H. Khan, and M. A. Haque, "Factors contributing to online child sexual abuse in Bangladesh: A qualitative inquiry," *F1000Research*, vol. 12, p. 1364, Aug. 2024, doi: 10.12688/f1000research.141568.3.
- [5] M. I. I. Towhid, R. Nuzhat, and M. A. Haque, "Protecting children from online sexual abuse in Bangladesh: A policy brief," *Bangabandhu Sheikh Mujib Medical University Journal*, vol. 16, no. 2, pp. 111-117, 2023, doi: 10.3329/bsmuj.v16i2.67209.
- [6] M. I. I. Towhid, *Digital Security Act 2018 and the draft Cyber Security Act 2023: A Comparative Analysis*, Position Paper, Transparency International Bangladesh, pp. 1-30, 2023, [Online]. Available: <https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf>.
- [7] M. S. Hossain and M. Mallika, "Cyber Security Governance Under the Cyber Laws of Bangladesh: An Overview," *International Journal of Research and Innovation in Social Science (IJRISS)*, vol. 9, no. 4, pp. 3796–3811, May 2025, doi: 10.47772/IJRISS.2025.90400271.



## PRIMARY SOURCES

1	<a href="#">banglajol.info</a> Internet Source	2%
2	Md. Rokonuzzaman Reza, Fabiha Mukarrama Binte Mannan, Dhrubo Barua, Shafayetul Islam, Nafiz Imtiaz Khan, Sharifa Rania Mahmud. "Developing a Machine Learning Based Support System for Mitigating the Suppression Against Women and Children", 2021 5th International Conference on Electrical Engineering and Information & Communication Technology (ICEEICT), 2021 Publication	1%
3	<a href="#">pmc.ncbi.nlm.nih.gov</a> Internet Source	1%
4	<a href="#">www.amnesty.org</a> Internet Source	1%
5	<a href="#">freedomhouse.org</a> Internet Source	1%
6	<a href="#">rsisinternational.org</a> Internet Source	1%
7	<a href="#">ecpat.org</a> Internet Source	<1%
8	Syed Toukir Ahmed Noor, Md. Fakrul Islam, Md Sabbir Hossain, Raisha Binte Islam et al. "The Association of Cyberbullying with Major Depressive Disorders among Bangladeshi Female Adolescents: Findings from the Bangladesh Adolescent Health and Wellbeing Survey 2019-20", Springer Science and Business Media LLC, 2025 Publication	<1%
9	<a href="#">lawyersclubbangladesh.com</a> Internet Source	<1%

10	asiafoundation.org Internet Source	<1 %
11	dergipark.org.tr Internet Source	<1 %
12	ourwork.sites.umassd.edu Internet Source	<1 %
13	Marium Salwa, Md Redwanul Islam, Mohammad Ibrahim Ibne Towhid, Anika Tasnim, Md Maruf Haque Khan, M Atiqul Haque. "Online child sexual abuse: a convergent parallel mixed-method exploration among Bangladeshi youth", BMJ Open, 2025 Publication	<1 %

---

Exclude quotes

On

Exclude bibliography

Off

Exclude matches

Off