P-ISSN 2664-0422	Pakistan Social Sciences Review	Nov-Dec 2026, Vol. 10, No. 6
O-ISSN 2664-0430	https://doi.org/10.35484/pssr.2026(10-VI)02	[23-42]

Pakistan Social Sciences Review
www.pssr.org.pk

RESEARCH PAPER

Smartphones, Social Media, and Silent Abuse: Cyberbullying and Digital Rights Violations among Bangladeshi Adolescents

Md. Ridwan
Assistant Professor, Department of Law, International Islamic University Chittagong, Bangladesh. https://orcid.org/0000-0002-8904-9956

Corresponding Author: ridwan-justice@iiuc.ac.bd

ABSTRACT

This article examines how cyberbullying and online abuse violate the rights of Bangladeshi adolescents and how the legal system has responded from the pandemic period to the present. Adolescents' smartphone and social media use has grown rapidly, yet online abuse remains widely under-reported. Cyber laws have been repeatedly amended without a child-specific protective framework. A qualitative socio-legal design combines doctrinal analysis of statutes and judgments with content analysis of documented cases from police, NGO and media sources. Cases are coded through the content, contact, conduct and contract risk typology and benchmarked against international child rights standards on the digital environment. Image-based sexual abuse, sextortion and AI-manipulated imagery dominate documented cases and are highly gendered. Peers increasingly perpetrate abuse. Laws criminalise harmful conduct but offer children few remedies. Stigma further silences victims. Bangladesh should adopt a rights-based child online safety law. Child-centred reporting, rapid takedown and school protocols are equally essential.

KEYWORDS Cyberbullying, Digital Rights, Adolescents, Bangladesh, General Comment No. 25, Image-Based Sexual Abuse

Introduction

In September 2020, a 16-year-old girl in Satkhira took her own life after a young man whose proposal she had refused carried out his threat to circulate fake, sexualised images of her on Facebook (The Business Standard, 2020a). In April 2025, police in Mongla reopened what had been recorded as an accidental death of a 14-year-old eighth-grader after her parents alleged she had been drugged, raped, filmed and then blackmailed with threats that the footage would be posted online and shown to her family (The Business Standard, 2025). In November 2026, students at a Dhaka school protested over allegations that a ninth-grade classmate had used artificial intelligence (AI) to fabricate obscene images of fellow students, and accused the school of intimidating those who spoke out (Daily Sun, 2026). These cases differ in their perpetrators, technologies and outcomes. They share a structure, however. A smartphone and a social media account became instruments of sexualised humiliation, the harm surfaced publicly only after it had become catastrophic or collective, and the institutions nearest to the child, the family, the school and the local police station, were slow, reluctant or complicit. This article calls that structure silent abuse.

Bangladesh's digital transformation makes the problem urgent. The Bangladesh Bureau of Statistics reports that individual internet use reached 59.2 per cent and mobile phone use 89.6 per cent of the population in April–June 2026 (United News of Bangladesh \[UNB\], 2026). A UNICEF-commissioned survey of 1,281 internet-using children aged 10–17 had already found in 2019 that 32 per cent were exposed to online violence,

OPEN ACCESS
© 2026 Author/s. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License (CC BY-NC 4.0).

cyberbullying or digital harassment, that a quarter first went online before age 11, and that 63 per cent used the internet mainly in their own rooms, a "bedroom culture" of largely unsupervised access (The Daily Star, 2019). More recent evidence links such exposure to serious harm. Among 4,984 female adolescents aged 15–19 in the nationally representative Bangladesh Adolescent Health and Wellbeing Survey, those who had been cyberbullied in the previous year were almost four times as likely to meet the threshold for major depressive disorder (Noor et al., 2025).

The law has moved quickly, but not in a child-centred direction. The Digital Security Act 2018 was replaced by the Cyber Security Act 2023, which the interim government repealed through the Cyber Security Ordinance 2025; the new parliament in turn replaced that Ordinance with the Cyber Security Act 2026 (Digibanglatech, 2026). Each iteration was debated primarily as a question of freedom of expression and state power over political speech (ARTICLE 19, 2025). Where children appeared at all, it was alongside women as subjects of sexual-content offences, not as rights-holders with distinct needs, including children harmed by other children in digital spaces. Meanwhile, the principal specialist reporting channel, the Police Cyber Support for Women, was established for female victims of cybercrime and has no dedicated child pathway (The Business Standard, 2020b).

This article argues that cyberbullying and online abuse of Bangladeshi adolescents are best understood not only as individual crimes or as a public-health risk but as **digital rights violations** for which the state, schools and platforms bear identifiable duties under the UN Convention on the Rights of the Child (UNCRC) and General Comment No. 25 on children's rights in relation to the digital environment (UN Committee on the Rights of the Child \[CRC\], 2021).

In doing so, the study adopts a precise understanding of who counts as an adolescent. Following the World Health Organization and the CRC's General Comment No. 20, adolescence is understood as the second decade of life (CRC, 2016). Because the Children Act 2013 defines every person under 18 as a child, the analysis concentrates on adolescents aged 10 to 17 years, who are developmentally adolescents and legally children. Data concerning 18- and 19-year-olds are drawn on only where they appear in aggregated national datasets, such as the 15–19 age band of the adolescent health survey, and are identified as such.

Against this background, the study is guided by three interrelated questions. It first asks what forms of cyberbullying and online abuse affecting Bangladeshi adolescents have been documented between 2020 and 2026, and how these forms map onto established typologies of online risk. Building on that mapping, it examines to what extent Bangladesh's legal and policy framework recognises, prevents and remedies these harms when assessed against the UNCRC and General Comment No. 25. Finally, it seeks to explain which social, institutional and platform-level factors keep this abuse silent, that is, unreported, unremedied and unaccounted for.

In pursuing these questions, the study sets out to map the documented forms of adolescent online abuse in Bangladesh using the 4Cs typology. It then subjects Bangladeshi law and policy to a doctrinal gap analysis against international child rights standards, and identifies the mechanisms through which victims are silenced. On that basis, it proposes a rights-based reform agenda addressed to the state, schools, platforms and the media.

The article proceeds as follows. It reviews the international and Bangladeshi literature, identifies the gap this study fills, sets out its theoretical framework and methodology, presents and discusses its findings through a harm–rights–response matrix, and closes with conclusions and recommendations.

Literature Review

Cyberbullying, online abuse and the problem of definition

Cyberbullying was initially conceptualised as an extension of school bullying, with its main elements being intentional, repeated aggression perpetrated via electronic communication, and the inability of the victim to escape the aggressor (Patchin&Hinduja, 2006; Smith et al., 2008). A later meta-analysis confirmed significant relationships between cyberbullying victimisation and depression, anxiety, suicidal thoughts and reduced engagement in school (Kowalski et al., 2014; Yaseen, et al.2026; Kaifa, et al. 2025). There has also been an argument against the analogy. Olweus (2012) has raised doubts about the existence of cyberbullying as a specific type of bullying, and feminist scholars have voiced concerns that the concept of 'bullying' downplays sexualised and gendered abuse. The term "technology-facilitated sexual violence" was coined by Henry and Powell (2018), and McGlynn et al. (2017) demonstrated that non-consensual creation and distribution of intimate imagery is a continuum of image-based sexual abuse that the term 'revenge porn' cannot capture. This online harassment is a civil rights issue that denies its victims (primarily women) access to public life, Citron (2014) argued. Dunn (2020) grouped them together as technology-facilitated gender-based violence.

This definitional debate matters for children. A peer posting a mocking meme, an adult extorting a 14-year-old with intimate images, and a classmate generating an AI "nude" all fall under the colloquial umbrella of cyberbullying in Bangladeshi public discourse. Yet they engage different rights, different laws and different institutional duties. This study therefore uses cyberbullying and online abuse as an inclusive term and disaggregates it analytically through the 4Cs typology discussed below.

Children's rights in the digital environment

A second literature reframes children's online experiences in rights terms. Livingstone and Third (2017) argued that debates had been dominated by protectionist anxieties that neglected children's rights to participation, expression and information. Third et al. (2019) traced how the UNCRC's provision, protection and participation rights apply online. This scholarship culminated in General Comment No. 25, which affirms that children's rights apply in the digital environment as they do offline and requires states to protect children from violence, exploitation and privacy violations while respecting their evolving capacities (CRC, 2021; Lansdown, 2005). Livingstone and Stoilova (2021) translated this agenda into the 4Cs typology of content, contact, conduct and contract risks, which links each type of harm to a different set of actors and remedies. Much of the effective "law" that regulates children online is found in platforms' terms of service and enforced through opaque moderation (Gillespie, 2018; Suzor, 2019).

The Bangladeshi evidence base

Bangladesh is experiencing uneven growth of research. Surveys record high exposure. The figure was 32 per cent of 10–17-year-olds, and 70 per cent of boys and 44 per cent of girls had accepted strangers as online friends, according to UNICEF's 2019

study (The Daily Star, 2019). Sarker and Shahid (2019) explored cyberbullying among high-school students aged 13–18 and found limited reporting to parents and schools. Haque et al. (2025), using mixed methods with grade 9–10 students, found that about 88 per cent of participants used the internet and over half reported some form of online sexual abuse; participants identified social media, chat groups and video games as the main avenues. Noor et al. (2025) provided the first nationally representative estimate for female adolescents, finding 8 per cent cyberbullying prevalence and a dose–response association with depression.

A larger body of work concerns young adults. Sheikh et al. (2023) documented substantial victimisation, fear and humiliation among 552 university students. Nova et al. (2019) showed how anonymous social media platforms were used for sexual harassment in Bangladesh's closely knit communal culture. Sambasivan et al. (2019), studying women in Bangladesh, India and Pakistan, identified cyberstalking, impersonation and leakage of personal content as dominant abuse types and found that victims coped through family and informal networks rather than formal reporting, because formal reporting risked reputational damage (Muzaffar, et al. 2019).

Institutional and civil-society data point the same way. The Cyber Crime Awareness Foundation's 2024 trend report found that three-quarters of surveyed victims were women and only 12 per cent reported incidents to law enforcement (The Financial Express, 2024). Between November 2020 and September 2024, the Police Cyber Support for Women received 40,280 complaints. Of the complainants, some 39 per cent did not proceed beyond initial intervention, and 41 per cent of complaints were about doctored images and personal details shared online (The Daily Star, 2024). Both datasets lack disaggregation by age, so the percentage of harms affecting children cannot be calculated, which is itself a gap in the evidence.

Legal scholarship and commentary

Legal commentary on Bangladesh's cyber laws has focused overwhelmingly on the misuse of the Digital Security Act 2018 and its successors against journalists, dissidents and online critics (ARTICLE 19, 2025). That critique is fair, but it has pushed aside discussion of the law's role in protecting children. Practitioner commentary has highlighted the cyber law's omission of bullying in private inboxes, where many cases of adolescent abuse take place (Dhaka Tribune, 2025), and the criminal justice system's lack of readiness to deal with AI-generated abuse (The Daily Star, 2025). The UN Committee on the Rights of the Child, in its most recent concluding observations on Bangladesh, raised concerns about violence against children and the implementation of the Children Act 2013 (CRC, 2015). These observations predate General Comment No. 25, however, and this study identified no subsequent review applying it to Bangladesh.

The literature review above identified four gaps that this study addresses.

First, most of the research in Bangladesh is quantitative and health-related. It determines prevalence and psychological correlates (Noor et al., 2025; Sheikh et al., 2023), but rarely examines the legal and institutional responses to abuse after it happens. Prevalence data cannot reveal whether a child's right to an effective remedy was respected.

Second, the highest-quality qualitative evidence relates to adult women and university students (Nova et al., 2019; Sambasivan et al., 2019; Salam, et. al. 2024;

Muzaffar, et al. 2020; Asghar, et al., 2025). The legal status of adolescents (under 18) is unique. They are children under the Children Act 2013, are subject to parental consent rules in data protection law, and may be both victims and offenders within the juvenile justice system. It is not possible to transpose evidence from adult women onto adolescents.

Third, Bangladeshi legal scholarship on cyber law has been dominated by the freedom-of-expression critique of successive security statutes (ARTICLE 19, 2025). The protective obligations the same statutes owe to children have received little doctrinal attention, and this study identified no published work assessing the post-2024 reforms, namely the Cyber Security Ordinance 2025, the Cyber Security Act 2026 and the new data protection regime, from a child rights perspective.

Fourth, although General Comment No. 25 was adopted in 2021, no Bangladesh-specific study appears to have used it asan evaluative benchmark. International research applying the 4Cs and General Comment No. 25 draws mainly on European and Anglophone contexts (Livingstone &Stoilova, 2021). How these frameworks operate where honour, shame and patriarchal family control shape both victimisation and reporting has not been examined.

By integrating doctrinal analysis with documented case evidence through a harm–rights–response matrix, this study connects what happens to adolescents online with what the law promises them and what institutions actually deliver.

Theoretical and Conceptual Framework

The study combines three lenses. Each answers a different question, and together they generate the harm–rights–response matrix used in the analysis.

Normative lens: children's rights in the digital environment

The normative benchmark is the UNCRC as interpreted by General Comment No. 25 (CRC, 2021). The analysis is organised around four aspects of the General Comment. First, it treats online rights as continuous with offline rights, meaning that the right to protection from all forms of violence (art.19), privacy (art.16) and protection from sexual exploitation (art.34) carry over to digital harms. Second, it places obligations on States to regulate businesses, such as platforms, so that they respect the rights of children by design. Third, it requires accessible and child-sensitive complaint and remedy mechanisms, recognising children's special needs in seeking remedies. Fourth, it demands a balance between protection, participation and evolving capacities, and warns against policies and practices that exclude children from digital life or criminalise them unnecessarily (Lansdown, 2005; CRC, 2016). All four follow the best-interests principle (CRC, 2013). This lens addresses which rights are engaged and who owes what duty.

Analytical lens: the 4Cs of online risk

The study adopts Livingstone and Stoilova's (2021) 4Cs typology of harms. Content risks are the potential for a child to come across unsuitable content. Contact risks arise when a child is targeted by an adult or an unknown person, as in grooming and sextortion. Conduct risks involve peer-to-peer interactions and can involve the child being a victim, a perpetrator or both. Contract risks arise from the child's relationship with commercial services, such as data exploitation and harmful design. The typology is important here because it distinguishes harms that are collapsed into the term

"cyberbullying" in public discourse in Bangladesh, and because each "C" refers to a different primary duty-bearer: content and contract to platforms and regulators, contact to law enforcement, conduct to schools, families and child-sensitive justice. This lens addresses what type of harm is involved.

Explanatory lens: the production of silence

The first two lenses cannot answer the question, "Why does so much abuse slip through the cracks and go unreported and unremedied?" The study therefore draws on three sociological concepts. Kelly's (1988) continuum of sexual violence shows how routine harassment and severe abuse form one spectrum, with the routine end being normalised, which is why it is rarely referred to as abuse. Goffman (1963) developed an account of stigma, a process that attaches stigma to the person depicted rather than to the person who created the image, thus providing a powerful incentive to conceal. Where a girl's reputation is tied to family honour, it is a rational choice for a family to keep silent, marry early or withdraw their child from school, in light of Kandiyoti's (1988) concept of patriarchal bargaining. This is what Sambasivan et al. (2019) report in their study of South Asian women's preferred coping styles. Combined, these ideas produce the study's central concept, "silent abuse" (online abuse where the social meaning assigns a penalty for disclosing it, so that a lack of disclosure reflects suppression rather than safety). This lens answers the question, "Why does the harm remain hidden?"

Conceptual model: the harm–rights–response matrix

The three lenses are translated into a three-column matrix: harm (as classified in the 4Cs), rights engaged (as listed in the UNCRC articles and General Comment No. 25 duties), and response (the applicable Bangladeshi law, the institutional response documented in cases, and the resulting gaps). Silence works as a mediating filter across the matrix that can obstruct the shift from harm to response at various points: disclosure, reporting, investigation, takedown and remedy. The matrix also draws on Bronfenbrenner's (1979) ecological perspective that the child's experience is influenced by nested systems. The microsystem, exosystem and macrosystem are represented by the family and school, the police and courts, and the law, platforms and gender norms, respectively. A rights violation can therefore arise at one layer and be exacerbated at another.

Methodology

Research design

This study adopts a qualitative socio-legal design combining doctrinal analysis of the laws and policies in Bangladesh with qualitative content analysis of documented cases of cyberbullying and online abuse of adolescents (2020–2026). The two strands are integrated through a harm–rights–response matrix, benchmarked against UNCRC General Comment No. 25.

The design is deliberately non-participatory. No data are collected directly from adolescents through surveys, interviews, focus groups or online observation, and no quantitative methods are used. This is because direct data collection is ethically problematic, as it risks re-traumatising child victims of sexualised abuse and because victims and families have shown documented reluctance to disclose (Sambasivan et al., 2019). It also reflects the research questions, which concern what the law offers and what institutions did – both of which are captured in documents. The socio-legal orientation

sees law as both text and practice, and explores the gap between legal promise and practice (Hutchinson & Duncan, 2012).

Strand A: Doctrinal analysis

The doctrinal strand examined primary and secondary legal sources in force or recently repealed during 2020–2026:

- **Constitutional provisions:** articles 27, 28(4), 32, 39 and 43 of the Constitution of Bangladesh.
- **Child-specific law:** the Children Act 2013 and the National Children Policy 2011.
- **Criminal and cyber law:** the Penal Code 1860, the Prevention of Oppression Against Women and Children Act 2000, the Pornography Control Act 2012, the Information and Communication Technology Act 2006, the Digital Security Act 2018, the Cyber Security Act 2023, the Cyber Security Ordinance 2025 and the Cyber Security Act 2026.
- **Data protection:** the Personal Data Protection Ordinance 2025 and its parliamentary successor.
- **Judicial guidance:** High Court Division directives on sexual harassment (BNWLA v. Government of Bangladesh, 2009).
- **International instruments:** the UNCRC, its Optional Protocol on the sale of children, child prostitution and child pornography, General Comments No. 13, 14, 20 and 25, and the Committee's concluding observations on Bangladesh (CRC, 2015).

The analysis proceeded in three steps: black-letter interpretation of each provision's scope, elements and remedies; a child-sensitivity assessment asking whether the provision recognises age, peer perpetration, privacy of child victims and access to remedy; and a gap analysis against the duties in General Comment No. 25.

Strand B: Qualitative content analysis of documented cases

Data sources. The documentary corpus comprised three source types:

1. **Reports in national daily newspapers**, in English and Bangla: The Daily Star, ProthomAlo, The Business Standard, Dhaka Tribune, The Financial Express, Daily Sun and bdnews24.com.
2. **Institutional and statistical sources:** Police Cyber Support for Women data as reported publicly, Bangladesh Bureau of Statistics ICT surveys, and UNICEF Bangladesh publications.
3. **Civil-society reports:** Cyber Crime Awareness Foundation trend reports and Cyber Support for Women and Children monitoring.

Search strategy. Newspaper archives and search engines were searched for 1 January 2020 to 15 November 2026. Searches combined English terms ("cyberbullying", "sextortion", "blackmail", "obscene photos", "deepfake", "Facebook", "schoolgirl",

"student", "minor") with Bangla equivalents (**সাইবারবুলিং**, **অনলাইনে হয়রানি**, **শিক্ষার্থী**, **কিশোরী**).

Inclusion criteria. Reports were included if they (a) described an identifiable incident or dataset concerning online abuse, (b) involved a victim or perpetrator stated to be aged 10–17 or described as a school pupil at secondary level or below, (c) concerned conduct in Bangladesh, and (d) reported at least one institutional response or the absence of one.

Exclusion criteria. Reports were excluded where the victim's age was unstated and could not be inferred from school grade, where the victim was 18 or older, where the account was opinion without factual reporting, or where the harm had no digital component. For example, a widely reported 2022 case concerning a college student whose private video circulated before her death was excluded because her age was not reported. Multiple reports of the same incident were merged into a single case record.

Coding and analysis

Case records were analysed using qualitative content analysis combining deductive and inductive coding (Hsieh & Shannon, 2005; Schreier, 2012). The deductive frame derived from the theoretical framework:

Table 1
Coding Framework for Documented Cases of Adolescent Cyberbullying and Online Abuse in Bangladesh

Dimension	Codes
Harm type (4Cs)	content; contact; conduct; contract
Modality	image-based abuse; sextortion; AI-manipulated imagery; impersonation or fake profile; verbal harassment; viral humiliation video
Perpetrator	peer (under 18); known adult; unknown adult; group
Rights engaged	UNCRC arts. 16, 19, 28, 34; General Comment No. 25 duties
Response	family; school; police; court; platform; none documented
Outcome	self-harm or suicide; school withdrawal; prosecution; diversion; takedown; unresolved

Inductive codes captured patterns not anticipated by the frame, such as initial misclassification of a death by police, institutional intimidation of complainants, and media disclosure of victims' identities. Coding was conducted in NVivo \[author to confirm software\]. A second coder independently coded a sample of \[author to insert: proportion\] of records, and discrepancies were resolved by discussion and recorded in a codebook audit trail.

Integration

The strands were integrated in a harm–rights–response matrix. For each harm category identified in Strand B, the matrix records the rights engaged, the applicable legal provisions identified in Strand A, the institutional responses documented in cases, and the resulting gap measured against General Comment No. 25. The matrix thereby connects documentary evidence of what happened with doctrinal evidence of what the law required. Throughout the results, documented facts are attributed to their sources, while interpretations are explicitly marked as the authors' analysis.

Trustworthiness and ethics

Credibility was supported by triangulating newspaper, institutional and civil-society sources, and dependability by a documented codebook and audit trail (Lincoln & Guba, 1985). Although all data are publicly available, the study follows ethical practice for research with documentary data on children (Bowen, 2009). No child victim is named in this article, even where the press published names, consistent with section 14 of the Prevention of Oppression Against Women and Children Act 2000 and section 81 of the Children Act 2013. Each case was checked, where possible, against at least two independent reports, and facts reported only as allegations are presented as allegations. Location is given only at district level, and verbatim quotation of social media content is avoided.

Limitations

Documented cases are a skewed sample. Media and institutional records over-represent severe outcomes, particularly suicide and criminal cases, as well as female victims and incidents that became public. Everyday peer harassment that never reaches a newspaper or police desk is under-represented, which is itself evidence of the silence the study examines. The study cannot estimate prevalence, and it reconstructs children's experiences from secondary accounts rather than their own voices. Finally, Bangladesh's legal framework changed several times during the study period. The doctrinal analysis reflects the texts as reported up to November 2026, and gazetted versions should be consulted for any later amendments.

Results and Discussion

The analysis produced five interlocking findings. The first three describe forms of harm. The last two concern the legal and social conditions that leave those harms unremedied. Table 1 summarises them in the harm–rights–response matrix.

Image-based sexual abuse and sextortion: the law arrives after the death

The most consistently documented harm affecting adolescent girls is the creation, threatened release or actual circulation of sexualised images, real or fabricated, typically by a male acquaintance. In the Satkhira case, the 16-year-old victim's uncle reported that the accused had long pursued her and threatened to post fake obscene photographs after she refused him. She died by suicide after the images spread on Facebook, and an arrest followed only afterwards (The Business Standard, 2020a). In the Mongla case, the 14-year-old victim was allegedly drugged, raped and filmed, then blackmailed with threats that the footage would be posted on Facebook and shown to her parents. Her death was first registered as accidental, and an FIR under the Prevention of Oppression Against Women and Children Act 2000 was recorded only after her parents petitioned the court (The Business Standard, 2025). Aggregated data, although not disaggregated by age, point in the same direction: 41 per cent of complaints to the Police Cyber Support for Women involved doctored images and personal details posted online, and a further 18 per cent involved blackmail with objectionable photographs (The Daily Star, 2024).

In 4Cs terms, these are **contact** harms when committed by adults and **conduct** harms when committed by peers or intimate partners. They engage the rights to privacy (art. 16), protection from violence (art. 19) and protection from sexual exploitation (art. 34). Doctrinally, Bangladeshi law is not empty here. The Pornography Control Act 2012 criminalises producing and distributing pornographic material and using it to humiliate or blackmail, the 2000 Act punishes sexual violence, and the Penal Code criminalises

abetment of suicide. **Our analysis suggests**, however, that the documented cases share a temporal pattern: the law was mobilised only after the harm had become irreversible. In neither case does the record show a preventive intervention, an emergency takedown or a protective order at the threat stage, even though, in the Satkhira case, the threat to circulate images was known to the family. General Comment No. 25 expects states to provide timely, child-sensitive mechanisms that can act before harm is complete. Bangladesh's framework is instead overwhelmingly punitive and retrospective. The Mongla case also shows that when a digital sex crime is prosecuted under general sexual violence law, the digital dimension (the footage, its copies and its removal) has no procedural home.

Synthetic imagery and peer perpetration: a juvenile justice problem disguised as a cybercrime problem

From 2025 the documented cases show a qualitatively new modality: AI-manipulated sexual imagery, in some cases produced by adolescents themselves. A coalition monitoring cyber violence recorded cases in the first half of 2025 that involved AI-generated fake nude images (Digibanglatech, 2025). Dhaka Tribune (2025) reported girls receiving manipulated images, known colloquially as gola-kata chobi ("cut-neck pictures"), in their inboxes. In Narayanganj, police investigating digitally altered obscene images of a young instructor found that several of the students responsible were minors. They were counselled and handed to their parents (The Daily Star, 2025). In November 2026, students at a Dhaka secondary school protested over allegations that a ninth-grader had used AI to create obscene images of classmates. They also alleged that the school barred ten protesting students from classes and examinations and locked students in a classroom to stop the demonstration (Daily Sun, 2026). These are allegations reported by the press, and this study makes no finding on their truth.

This is a **conduct** risk with a **contract** dimension, since it depends on consumer AI tools and platforms that permit their outputs to circulate. Peer perpetration creates a doctrinal tension the current framework does not resolve. The Cyber Security Ordinance 2025 criminalised harmful material generated or edited using AI (The Daily Star, 2025), and Parliament later amended the cyber security law to enable swift removal of harmful AI-generated content (Bangladesh Sangbad Sangstha \[BSS\], 2026). Neither instrument, as reported, distinguishes child offenders. The Children Act 2013 provides diversion and child-sensitive procedures for children in conflict with the law, and General Comment No. 24 favours non-custodial, restorative responses (CRC, 2019). The Narayanganj outcome, counselling and parental hand-over, looks like informal diversion, but **in our reading** it occurred outside any documented procedure, without any reported remedy for the victim beyond the removal of the images.

Schools are the missing duty-bearer. The High Court Division's guidelines in BNWLA v. Government of Bangladesh (2009) require educational institutions to establish complaint committees for sexual harassment, and they extend protection to girls and children as well as women. Their definition of sexual harassment expressly includes insult through letters, telephone and cell phone calls, and SMS. If the Dhaka allegations are substantiated, a school that disciplined complainants rather than convening such a committee would have inverted that duty. This illustrates why, under General Comment No. 25, the conduct domain demands institutional protocols and not only criminal provisions.

Viral humiliation: offline violence, digital amplification

A third pattern concerns offline abuse that becomes a digital harm through recording and sharing. In Gopalganj in July 2026, a 13-year-old eighth-grader and a young man were allegedly tied to a tree inside a school compound and humiliated in front of teachers, students and residents. Onlookers filmed the incident, the video spread on Facebook, and the girl's family reported that she then attempted suicide. Three days later the officer-in-charge of the local police station said no complaint had been filed and that action would follow if one were received, while the headmaster deferred action pending consultation with the managing committee (ProthomAlo, 2026).

This case combines a **content** harm (circulation of humiliating footage of a child) with **conduct** by adult bystanders who filmed rather than intervened. **We interpret** it as the clearest instance of silent abuse in the corpus. The abuse was public, yet the institutions treated it as private. The state's duty under article 19 UNCRC, elaborated in General Comment No. 13, is one of due diligence: to prevent, investigate and respond to violence against children, not merely to await a complaint (CRC, 2011). Policing that waits for a complaint shifts the burden of initiating justice onto a 13-year-old and her family at the moment of maximum stigma. No platform takedown of the video is reported.

A fragmented and child-blind legal architecture

The doctrinal analysis shows a framework that is dense but poorly designed for children. Three features stand out.

First, **legislative churn**. Four principal cyber statutes or ordinances operated within eight years (2018, 2023, 2025 and 2026), and the three reforms since 2023 were driven primarily by concerns about the earlier laws' use against political speech (ARTICLE 19, 2025; Digibanglatech, 2026). That focus was justified. Its by-product, however, was that protective provisions were drafted and redrafted with little attention to children. During the 2025 redrafting a general cyberbullying clause was removed while offences against women and children were added (Views Bangladesh, 2025), leaving peer harassment that is not sexual in content without a clear statutory home. Practitioners have also noted that the cyber law did not reach bullying in private inboxes (Dhaka Tribune, 2025).

Second, **no child-specific online protection instrument**. The Children Act 2013 contains no provisions addressing online abuse. Offences relevant to children are scattered across at least five statutes, none of which requires child-sensitive investigation of digital evidence, rapid takedown for child victims, or protection of child victims' identities in online reporting.

Third, the **data protection regime** is the most child-attentive recent development. The Personal Data Protection Ordinance 2025 required parental or guardian consent for processing children's data and prohibited profiling, behavioural tracking and targeted advertising directed at minors (BSS, 2025). According to a former special assistant to the Chief Adviser, the parliamentary successor law made processing of children's data for AI training a criminal offence, but did not retain some of the ordinance's criminal provisions for large-scale privacy violations (Digibanglatech, 2026). The same commentator has alleged that Meta repeatedly lobbied to lower the age threshold for children from 18 (Taiyeb, 2026). That account is an opinion piece and is cited here as a reported claim, not an established fact. If accurate, it shows that the **contract** domain is

shaped by contested negotiation between the state and platforms. General Comment No. 25 resolves that contest in favour of children's best interests.

Table 2
Harm–rights–response matrix (authors' synthesis)

Harm (4Cs)	Rights engaged	Main legal response	Documented institutional response	Gap against General Comment No. 25
Image-based abuse and sextortion (contact/conduct)	arts. 16, 19, 34	Pornography Control Act 2012; 2000 Act; Penal Code; cyber law	Arrest or FIR after death; initial misclassification	No preventive or takedown mechanism; no child pathway
AI-manipulated imagery by peers (conduct/contract)	arts. 16, 19, 34, 40	AI provisions in cyber law; Children Act 2013	Informal counselling; alleged school retaliation	No diversion protocol; no school duty specific to digital abuse; no victim remedy
Viral humiliation video (content/conduct)	arts. 16, 19, 28	General criminal law; HCD guidelines (2009)	Police awaiting complaint; school inaction	Due diligence unmet; no platform takedown
Data exploitation and profiling (contract)	arts. 3, 16, 17	Data protection ordinance and successor law	Not yet tested in reported cases	Enforcement authority still to be established
Peer harassment in private messaging (conduct)	arts. 16, 19, 29	Unclear after removal of cyberbullying clause	Rarely documented	Legal vacuum; reliance on family coping

The production of silence

The final finding concerns why abuse remains unreported. Three mechanisms recur across the corpus.

Reputational risk to the family. Consistent with Goffman's (1963) account of stigma and Kandiyoti's (1988) patriarchal bargaining, a sexualised image, real or fabricated, discredits the girl and her family rather than the perpetrator. The Satkhira and Mongla cases became public only through death; in Mongla, the family learned of the abuse only afterwards. In both, disclosure came only when silence could no longer protect anyone.

Institutional attrition. Even when victims come forward, many withdraw. Some 39 per cent of Police Cyber Support for Women complainants did not proceed beyond initial intervention. A women lawyers' association leader attributed this to the absence of victim-centric support, and police cited fear of exposure (The Daily Star, 2024). Only 12 per cent of victims surveyed by the Cyber Crime Awareness Foundation reported to law enforcement (The Financial Express, 2024). Lawyers have described the justice system as unprepared for AI-enabled abuse, with forensic evidence optional and screenshots routinely accepted (The Daily Star, 2025). None of these channels is designed for a 14-year-old, who must ordinarily act through a parent who may be the person she most fears telling.

Secondary exposure through reporting. Several of the news reports examined named child victims and their villages. Section 14 of the Prevention of Oppression Against Women and Children Act 2000 prohibits disclosure of the identity of victims of offences under that Act, and the High Court Division has barred the media from publishing the photographs and identities of rape victims (The Business Standard, 2021).

Section 81 of the Children Act 2013 further restricts publication of information relating to proceedings under that Act in print, electronic and online media. General Comment No. 25 likewise calls for protection of children's privacy in the digital environment. **We suggest** that media practice which re-identifies child victims online reproduces the very harm being reported and deters future disclosure.

Taken together, these mechanisms support the study's central claim. The low volume of formal complaints by adolescents is not evidence of low victimisation. It is better read as an indicator of suppression, consistent with survey evidence that around a third of 10–17-year-olds face online harassment (The Daily Star, 2019) and that its mental-health consequences are severe (Noor et al., 2025). The harm–rights–response matrix shows that the gap does not lie mainly in the absence of criminal offences. It lies in the absence of child-centred procedure: prevention at the threat stage, accessible reporting, rapid takedown, school accountability, diversion for child perpetrators, and remedy for child victims.

Conclusion

This article set out to determine what forms of online abuse Bangladeshi adolescents experience, how far the law answers them, and why so much of that abuse remains hidden. Three conclusions follow.

First, the harms documented between 2020 and 2026 are dominated by sexualised, image-based abuse that is highly gendered and increasingly synthetic. The arrival of consumer AI tools has shifted part of the threat from adult acquaintances and strangers to classmates, turning what was framed as a cybercrime problem into a question of juvenile justice and school governance as well.

Second, Bangladesh does not lack criminal offences. It lacks child-centred procedure. Successive cyber laws were reformed, legitimately, to curb the suppression of speech, but children were largely absent from those debates. The result is a framework that punishes after the fact but offers few means to prevent circulation at the threat stage, remove content quickly, involve schools, divert child offenders or provide remedies to child victims. The data protection regime is the notable exception, and its child-specific safeguards now need an enforcement authority to give them effect.

Third, silence is produced, not natural. Family honour, institutional attrition, reactive policing and media re-identification work together so that harm reaches the formal system mainly when it has become catastrophic. Measured against General Comment No. 25, the core failure is therefore procedural and institutional rather than legislative in the narrow sense.

The study's contribution is twofold. Empirically and doctrinally, it offers, to our knowledge, the first child rights assessment of Bangladesh's post-2024 cyber and data protection reforms. Conceptually, it proposes the harm–rights–response matrix and the construct of silent abuse as tools that other jurisdictions with strong honour norms and rapid smartphone adoption can apply. Future research should build on this documentary foundation with ethically designed, child-participatory work, for instance through child rights impact assessments, once safe and trauma-informed conditions are in place.

Recommendations

The recommendations follow directly from the gaps identified in the matrix and are addressed to specific duty-bearers.

For Parliament and the Ministry of Law

- **Enact a child online safety framework**, either as a dedicated statute or as a digital chapter in the Children Act 2013. It should define cyberbullying and image-based abuse of children (including AI-generated imagery), provide for emergency protection and takedown orders at the threat stage, and expressly integrate General Comment No. 25.
- **Restore a clear legal home for non-sexual peer harassment**, including in private messaging, while ensuring that any offence is narrowly drafted so that it cannot be misused against legitimate expression.
- **Mandate diversion and restorative procedures for child perpetrators** of digital abuse under the Children Act 2013, paired with enforceable remedies, such as removal, apology, counselling and compensation, for child victims.

For the Ministry of Home Affairs and the police

- **Create a dedicated child pathway** within the Police Cyber Support for Women or a new child cyber desk, accessible directly to adolescents through the national child helpline 1098, with trained female and child-specialist officers and the power to request urgent platform takedowns.
- **Adopt a due-diligence standard** under which police open an inquiry into publicly circulating abuse of a child without waiting for a family complaint, and require forensic preservation of digital evidence rather than reliance on screenshots.

For the Ministry of Education, schools and madrasas

- **Operationalise the High Court Division's 2009 guidelines** by requiring every secondary institution to maintain a functioning complaint committee whose mandate expressly covers digital and AI-generated abuse, with a prohibition on retaliation against complainants.
- **Integrate digital rights and consent education** into the national curriculum, addressing image sharing, AI manipulation and bystander responsibility.

For regulators and platforms

- **Establish the data protection authority promptly** and prioritise enforcement of the bans on profiling and targeted advertising directed at children.
- **Require platforms operating in Bangladesh to provide Bangla-language, child-specific reporting tools**, publish country-level transparency data on child-related takedowns, and conduct child rights impact assessments for AI image tools.

For the media

- **Adopt and enforce a press code** that prohibits identifying child victims by name, school or village, consistent with section 14 of the Prevention of Oppression Against Women and Children Act 2000 and section 81 of the Children Act 2013.

Taken together, these measures would shift Bangladesh's response from punishment after catastrophe to protection before harm, which is the move General Comment No. 25 requires.

Declarations

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Ethical Considerations

No human subjects or personal information was used in this study. It is based exclusively on published books that are accessible to the public (and publisher descriptions and epitexts) cited in the references. Ethical approval was not necessary.

AI Use Statement

Generative AI (ChatGpt and Grammarly) was used for language editing and condensing text. It was not used for the data collection, coding the corpus and drawing findings. All text generated by AI is reviewed and edited by the author, and the author is responsible for the article's content.

Data Availability Statement

The data analysed are all published data, as mentioned in the references. The 39 corpus books are listed verifying, with the verification sources. The coding frame and coded dataset are available on reasonable request from the author.

References

ARTICLE 19. (2025). ARTICLE 19 calls for meaningful consultation on draft Cyber Protection Ordinance 2025 \[Press statement\]. https://article19.org/wp-content/uploads/2025/02/ARTICLE-19-Press-statement-on-draft-cyber-protection-ordinance-2025_DvdG.pdf

Asghar, N., Cheema, A. T., & Muzaffar, M. (2025). The Impact of Media Coverage on Political Behavior among Pakistani Students: A Case Study of GC Women University Sialkot. *Journal of Development and Social Sciences*, *6*(2), 266–279. https://doi.org/10.47205/jdss.2025(6-II)23

Bangladesh National Women Lawyers Association v. Government of Bangladesh, Writ Petition No. 5916 of 2008 (High Court Division, Supreme Court of Bangladesh, May 14, 2009).

Bangladesh Sangbad Sangstha. (2025, November 9). Govt issues gazettes of 2 landmark ordinances on data protection, governance. https://www.bssnews.net/news-flash/330104

Bangladesh Sangbad Sangstha. (2026, June 30). Cyber Security Amendment Bill, 2026 passed in JS. https://www.bssnews.net/js-session/401310

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27–40. https://doi.org/10.3316/QRJ0902027

Bronfenbrenner, U. (1979). The ecology of human development: Experiments by nature and design. Harvard University Press.

Children Act, 2013 (Act No. 24 of 2013) (Bangladesh).

Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.

Constitution of the People's Republic of Bangladesh, 1972.

Convention on the Rights of the Child, November 20, 1989, 1577 U.N.T.S. 3.

Cyber Security Act, 2023 (Bangladesh).

Cyber Security Act, 2026 (Bangladesh).

Cyber Security Ordinance, 2025 (Ordinance No. 25 of 2025) (Bangladesh).

Daily Sun. (2026, November 3). Udayan School students protest over sexual harassment allegations. https://www.daily-sun.com/bangladesh/906971

Dhaka Tribune. (2025, March 8). Deepfake: Trapped in a digital nightmare. https://www.dhakatribune.com/bangladesh/375687/deepfake-trapped-in-a-digital-nightmare

Digibanglatech. (2025, July 8). Cyber violence climbing: AI-driven abuses target women and children in Bangladesh. https://digibanglatech.news/155420

Digibanglatech. (2026, April 11). Cyber security statute strengthened: Parliament passes Cyber Security Bill-2026. https://digibanglatech.news/173569

Digital Security Act, 2018 (Act No. 46 of 2018) (Bangladesh).

Dunn, S. (2020). Technology-facilitated gender-based violence: An overview (Supporting a Safer Internet Paper No. 1). Centre for International Governance Innovation.

Gillespie, T. (2018). Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media. Yale University Press.

Goffman, E. (1963). Stigma: Notes on the management of spoiled identity. Prentice-Hall.

Haque, M. A., Salwa, M., Islam, M. R., Towhid, M. I. I., Tasnim, A., & Khan, M. M. H. (2025). Online child sexual abuse: A convergent parallel mixed-method exploration among Bangladeshi youth. BMJ Open, 15(5), Article e091042. https://doi.org/10.1136/bmjopen-2024-091042

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208. https://doi.org/10.1177/1524838016650189

Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. Qualitative Health Research, 15(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art70

Information and Communication Technology Act, 2006 (Act No. 39 of 2006) (Bangladesh).

Kaifa, U., Yaseen, Z. & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications, *Journal of Climate and Community Development, 4*(1), 39-54.

Kandiyoti, D. (1988). Bargaining with patriarchy. Gender & Society, 2(3), 274–290. https://doi.org/10.1177/089124388002003004

Kelly, L. (1988). Surviving sexual violence. Polity Press.

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., &Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. Psychological Bulletin, 140(4), 1073–1137. https://doi.org/10.1037/a0035618

Lansdown, G. (2005). The evolving capacities of the child. UNICEF Innocenti Research Centre.

Lincoln, Y. S., & Guba, E. G. (1985). Naturalistic inquiry. SAGE.

Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. New Media & Society, 19(5), 657–670. https://doi.org/10.1177/1461444816686318

Livingstone, S., &Stoilova, M. (2021). The 4Cs: Classifying online risk to children (CO:RE Short Report Series on Key Topics). Leibniz-InstitutfürMedienforschung | Hans-Bredow-Institut. https://doi.org/10.21241/ssoar.71817

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond "revenge porn": The continuum of image-based sexual abuse. Feminist Legal Studies, 25(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2

Ministry of Women and Children Affairs. (2011). National children policy 2011. Government of the People's Republic of Bangladesh.

Muzaffar, M., Chohdhry, S., & Afzal, N. (2019). Social Media and Political Awareness in Pakistan: A Case Study of Youth, *Pakistan Social Sciences Review*, 3 (II), 1-13

Muzaffar, M., Yaseen, Z. & Safdar, S. (2020). Role of Social Media in Political Campaigns in Pakistan: A Case of Study of 2018 Elections*, Journal of Political Studies, 27* (2), 141-151

Noor, S. T. A., Islam, M. F., Hossain, M. S., Islam, R. B., Banik, R., Islam, S., Sarker, S., Nasrullah, M., & Raza, S. (2025). 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, 25, Article 783. https://doi.org/10.1186/s12888-025-07234-z

Nova, F. F., Rifat, M. R., Saha, P., Ahmed, S. I., &Guha, S. (2019). Online sexual harassment over anonymous social media in Bangladesh. In Proceedings of the Tenth International Conference on Information and Communication Technologies and Development (ICTD '19) (Article 1, pp. 1–12). Association for Computing Machinery.

Olweus, D. (2012). Cyberbullying: An overrated phenomenon? European Journal of Developmental Psychology, 9(5), 520–538. https://doi.org/10.1080/17405629.2012.682358

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, A/RES/54/263.

Patchin, J. W., &Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. Youth Violence and Juvenile Justice, 4(2), 148–169. https://doi.org/10.1177/1541204006286288

Penal Code, 1860 (Act No. XLV of 1860) (Bangladesh).

Personal Data Protection Ordinance, 2025 (Bangladesh).

Pornography Control Act, 2012 (Act No. 9 of 2012) (Bangladesh).

Prevention of Oppression Against Women and Children Act, 2000 (Act No. 8 of 2000) (Bangladesh).

ProthomAlo. (2026, August 1). Schoolgirl attempts suicide after being tied to a tree and tortured in Gopalganj. https://en.prothomalo.com/bangladesh/local-news/v9umvq0cw1

Salam, Z., Jamil, M., & Muzaffar, M. (2024). The Role of Social Media in Political Awareness and Engagement among University Students: A Quantitative Study. *Journal of Development and Social Sciences*, *5*(4), 691–702. https://doi.org/10.47205/jdss.2024(5-IV)61

Sambasivan, N., Batool, A., Ahmed, N., Matthews, T., Thomas, K., Gaytán-Lugo, L. S., Nemer, D., Bursztein, E., Churchill, E., &Consolvo, S. (2019). "They don't leave us alone anywhere we go": Gender and digital abuse in South Asia. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (Paper 2, pp. 1–14). Association for Computing Machinery. https://doi.org/10.1145/3290605.3300232

Sarker, S., &Shahid, A. R. (2019). Cyberbullying of high school students in Bangladesh: An exploratory study (arXiv:1901.00755). arXiv. https://arxiv.org/abs/1901.00755

Schreier, M. (2012). Qualitative content analysis in practice. SAGE.

Sheikh, M. M. R., Hossan, M. R., &Menih, H. (2023). Cyberbullying victimization and perpetration among university students in Bangladesh: Prevalence, impact and help-seeking practices. Journal of School Violence, 22(2), 198–214. https://doi.org/10.1080/15388220.2023.2168681

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., &Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Suzor, N. P. (2019). Lawless: The secret rules that govern our digital lives. Cambridge University Press.

Taiyeb, F. A. (2026, March 14). The business of child data profiling: Why did Meta exert undue pressure on the Data Protection Ordinance? The Business Standard. https://www.tbsnews.net/node/1386956

The Business Standard. (2020a, September 12). One arrested over spreading illicit photos of a girl on Facebook. https://www.tbsnews.net/bangladesh/crime/one-arrested-over-spreading-illicit-photos-girl-facebook-131800

The Business Standard. (2020b, November 16). Police cyber support unit received 25 complaints within 6 hours of launch. https://www.tbsnews.net/bangladesh/crime/police-cyber-support-unit-received-25-complaints-within-6-hours-launch-158860

The Business Standard. (2021). HC bars media from publishing photos, identities of rape victims. https://www.tbsnews.net/bangladesh/hc-bars-media-publishing-photos-identities-rape-victims-213100

The Business Standard. (2025, April 25). 'Drugged, raped, filmed': Youth arrested for 'instigating 8th grader's suicide' with repeated abuse.

https://www.tbsnews.net/bangladesh/crime/drugged-raped-filmed-youth-arrested-instigating-8th-graders-suicide-repeated-abuse

The Daily Star. (2019, February 6). Cyber safety in Bangladesh: 32pc children bullied online. https://www.thedailystar.net/country/safer-internet-day-2019-prevent-bullying-of-children-online-in-bangladesh-unicef-1697785

The Daily Star. (2024). Cybercrimes continue to scourge women. https://www.thedailystar.net/node/3743096

The Daily Star. (2025, November 30). 16 days of activism: AI fuelling cyber violence against women\[N. Jahan, Reporter\]. https://www.thedailystar.net/news/bangladesh/news/16-days-activism-ai-fuelling-cyber-violence-against-women-4047706

The Financial Express. (2024, June 29). Social media and online account hacking most prevalent cybercrime in Bangladesh: Study.

Third, A., Livingstone, S., & Lansdown, G. (2019). Recognizing children's rights in relation to digital technologies: Challenges of voice and evidence, principle and practice. In B. Wagner, M. C. Kettemann, & K. Vieth (Eds.), Research handbook on human rights and digital technology (pp. 376–410). Edward Elgar.

UN Committee on the Rights of the Child. (2011). General comment No. 13 (2011): The right of the child to freedom from all forms of violence (CRC/C/GC/13).

UN Committee on the Rights of the Child. (2013). General comment No. 14 (2013) on the right of the child to have his or her best interests taken as a primary consideration (CRC/C/GC/14).

UN Committee on the Rights of the Child. (2015). Concluding observations on the fifth periodic report of Bangladesh (CRC/C/BGD/CO/5).

UN Committee on the Rights of the Child. (2016). General comment No. 20 (2016) on the implementation of the rights of the child during adolescence (CRC/C/GC/20).

UN Committee on the Rights of the Child. (2019). General comment No. 24 (2019) on children's rights in the child justice system (CRC/C/GC/24).

UN Committee on the Rights of the Child. (2021). General comment No. 25 (2021) on children's rights in relation to the digital environment (CRC/C/GC/25).

United News of Bangladesh. (2026). Mobile phone ownership rises: BBS. https://unb.com.bd/category/Bangladesh/mobile-phone-ownership-rises-bbs/195830

Views Bangladesh. (2025). Draft Cyber Security Ordinance makes cybercrime against women, children punishable.

Yaseen, Z., Muzaffar, M. Asghar, N., & Fatima, A. (2026). Artificial Intelligence as a Predictor of Cybersecurity Awareness among University Students: A Quantitative Study. (2026). *Journal of Politics and International Studies*, *12*(1), 200–220