**Asia Internet Coalition (AIC) Industry Submission on The Draft Cyber Security Act, 2023, Bangladesh**

---

**29 August 2023**

To

Mr. Zunaid Ahmed Palak
Minister of State, Information, Communication and Technology Division Ministry of Posts, Telecommunications and Information Technology People's Republic of Bangladesh
Dhaka, Bangladesh

Dear State Minister Palak,

On behalf of the Asia Internet Coalition ("AIC") and its members, I am writing to express our sincere gratitude to the Information and Communication Technology Division for leading the drafting process of the new Cyber Security Act 2023 and for the opportunity to submit comments on the latest draft published on, 2023 (the "August 2023 Draft" or "Draft Act"). AIC is an industry association of leading internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of internet and information and communication technology policy issues, and are fully committed to the cause of a safe and open internet.

**Executive Summary**

We support the efforts made by the government of Bangladesh in drafting the Cyber Security Act 2023 (CSA) with the aim of creating legislation in line with constitutional principles of freedom of expression and global best practices and standards, which the international community and industry has long called for. It is important to note that well designed regulation and frameworks can foster a productive digital environment in Bangladesh that upholds fundamental rights, encourages innovation, and ensures online safety, which will facilitate a thriving ecosystem for new business investments. On the other hand, regulations that are broad, ambiguous, and unclear risk government overreach and misuse and potentially lead to unintended and adverse consequences that might make people less safe online, stifle free expression, slow innovation, and impact future business opportunities.

The draft regulation has several areas that are of concern to the industry members and are discussed in detail below. In summary, the proposed regulatory framework lacks clear and precise definitions, a robust safe harbour framework, unreasonable and disproportionate employee liability, and a lack of procedural safeguards. Further, the process in which the CSA was developed and released did not involve a comprehensive legislative consultation process.

1. **Broad and ambiguous categories and definitions of unlawful content.** The categories of unlawful content outlined in the draft CSA are broad and ambiguous and may be susceptible to misuse. Furthermore, the categories and definitions of illegal content are inconsistent with international human rights standards, including the

International Covenant on Civil and Political Rights (ICCPR), which Bangladesh has signed and ratified.

2. **Lack of adequate safe harbour.** Obligations on intermediary service providers are overbroad and unclear without adequate safeguards, which creates an unpredictable liability regime.
3. **Disproportionate liability for employees.** Disproportionate criminal liability for employees is contrary to international standards and creates and unfavourable environment for foreign direct investment.
4. **Lack of proper procedural safeguards.** Lack of clarity on whether BTRC will act as the sole authority for takedown requests , as well as lack of due process requirements (including duly-reasoned court orders)
5. **Lack of a meaningful and comprehensive consultation process.** To ensure effective and far regulation, it is crucial to engage in informed and iterative consultations with a wide ranging stakeholders. Ensuring broad participation from relevant stakeholders in the government, civil society, academia, digital platforms, etc,… with sufficient time to respond is proven to be effective, rendering consultations collaborative, ongoing, public and transparent.

We therefore request that the Bangladesh government consider the issues highlighted in this submission and provide the AIC an opportunity for further engagement and consultation on the CSA.

| Section | Recommendations |
|---|---|
| 21 (1)<br>**Punishment for any propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag.—** (1) If any person, by means of digital or electronic medium, makes or instigates to make any propaganda or campaign against the liberation war of Bangladesh, spirit of liberation war, father of the nation, national anthem or national flag, then such act of the person shall be an offence. | Absent specific definitions, the terms are subject to broad interpretation resulting in (a) over censorship and regulatory overreach, (b) selective, arbitrary and/or disproportionate enforcement actions, (c) overcriminalization, and (d) restricting free speech.<br><br>It is unclear as to what constitutes "propaganda" and "campaign". Similarly , the definition of "affect the image or reputation of the country, or to speed confusion" is unclear.<br><br>We would like to stress that eliminating superfluous definitions will improve implementation. The above-mentioned phrases are broad and capable of being misinterpreted/misused. These terms should be narrowly defined to avoid regulatory overreach.<br><br>Categories and definitions for unlawful content should be clear, precise, operable and publicly explainable to ensure consistent application of the law. Broad and ambiguous definitions would result in inconsistent application and uncertainty on what is prohibited that could lead to over-censorship both for platforms and users themselves.<br>The Siracusa Principles, under the International Covenant on Civil and Political Rights (ICCPR), which Bangladesh has signed and ratified, state that restrictions on human |
| 25 (1) (b)<br>**Transmission, publication, etc. of offensive, false or threatening data-information.—** (1) If any person, through any website | |

| Section | Recommendations |
|---|---|
| or any other digital or electronic medium,—<br>(b) publishes or propagates, or abets to publish or propagate, any information, as a whole or partly, which he knows to be propaganda or false, with an intention to affect the image or reputation of the country, or to spread confusion, | rights must meet standards or legality, evidence-based necessity, proportionality , and gradualism.<br><br>In coming to a decision regarding whether restricting or removing content is proportionate, we recommend that following tests be considered to ensure adherence with international human rights obligations:<br>- Prevalence: the number of people affected or likely to be affected by the content.<br>- Severity: the degree of real-world harm caused or likely to be caused to the people affected.<br>- Urgency: the immediacy of the harm or threatened harm.<br>- Discrimination: whether takedown demands target particular population groups on the basis of race, religion, gender, sexual orientation or other protected categories. |
| 25 (1) (a)<br>**Transmission, publication, etc. of offensive, false or threatening data-information.**— (1) If any person, through any website or any other digital or electronic medium,—<br>(a) intentionally or knowingly transmits, publishes or propagates any data- information which he knows to be offensive, false or threatening in order to annoy, insult, humiliate or malign a person; or | We recommend deletion of this clause. The terms "offensive", "threatening" "in order to annoy" introduce subjectivity in content assessments, which would result in (a) over censorship and regulatory overreach, (b) selective, arbitrary and/or disproportionate enforcement actions, (c) overcriminalization, and (d) restricting free speech.<br><br>Retaining this provision allows potential abuse as user generated content may be deemed offensive, false or threatening, irrespective of the intention of the user. In fact, contrary to constitutional law and criminal law principles, inclusion of such a provision may result in "assumed" intent. |
| 2 (1) (s)<br>**Definitions.**— (1) In this Act, unless there is anything repugnant in the subject or context—<br>**"defamation"** means defamation as defined under section 499 of the Penal Code (Act XLV of 1860); | Definition of "defamation" is too broad, as it includes (a) sarcastic and ironic statements, and (b) direct or indirect imputations which (on a subjective assessment) lowers the character or credit of an individual.<br><br>We recommend limiting the definition of "defamation" to false content that intentionally communicated to another with an intent to defame and cause damage. Content that is manifestly made in sarcastic contexts should also be excluded from the definition.<br>Further content deemed as "defamation" should only be actionable by service providers if accompanied by a court order. |

| Section | Recommendations |
|---|---|
| 2 (1) (w)<br>**"service provider"** means – –<br>(i) any person who enables any user to communicate through computer or digital process; or<br>(ii) any person, entity or institution who or which processes or preserves computer data in favour of the service or the user of the service. | As currently drafted, the provision is overly broad, which will create unpredictability in the application of the Act.<br><br>We request clarity that the definition applies only to intermediary service providers that enable users to publicly post, create, publish or share content to a broad audience and third-party user engagement. Private communications, such as via one-to-one messaging services, should be excluded. |
| 4. Extra-territorial application of the Act | At present this clause offers a very broad extraterritorial effect with seemingly no need for a nexus with Bangladesh. We would request language specifying that, when it comes to seeking data from service providers based outside of Bangladesh, law enforcement agencies should follow established procedures of international law -- including treaty-based and other diplomatic procedures. |
| 29<br><br>**Publication, transmission etc. of defamatory information.—** If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) on website or any other electronic format, he shall be punished with a fine not exceeding 25 (twenty-five) lac taka.<br><br>28 (1)<br>**Publication, broadcast, etc. of information on website or electronic format that hurts the religious values or sentiment.—** (1) If any person or group willingly or knowingly publishes or broadcasts, or causes to publish or broadcast, anything in website or any | These clauses essentially treat transmission as an offence. Overly broad clauses like these could potentially impose liability on intermediaries in the absence of malicious intent. This could prevent intermediaries from delivering services to users in Bangladesh.<br><br>Absent express *mens rea* requirement, a service provider transmitting the content without criminal intent could be prosecuted. We therefore request clarity that transmission by intermediary service providers unintentionally will not constitute an offence. |

| Section | Recommendations |
|---|---|
| electronic format which hurts religious sentiment or values, with an intention to hurt or provoke the religious values or sentiments, then such act of the person shall be an offence. | |
| 35(1)<br>**Offence committed by a company.—** (1) Where an offence under this Act is committed by a company, every owner, chief executive, director, manager, secretary, partner or any other officer or employee or representative of the company who has direct involvement with the offence shall be deemed to have committed the offence, unless he proves that the offence was committed without his knowledge or he tried his best to prevent the offence. | We recommend deletion of this provision.<br>Corporate actions involve numerous individuals and systemic factors, which makes attributing criminal liability to a single person unreasonable and disproportionate. Consistent with established principles of criminal law, individuals should not be "deemed" to have committed an offence.<br><br>This provision creates vicarious liability for individuals associated with a non-compliant company (even if inn representative capacity)), unless they are able to prove that they were unaware of the violation or did all they could to prevent it. It reverses the burden of proof and presumption of innocence.<br><br>Use of phrases like "direct involvement" and "tried his best to prevent the offence " (or "exercised all due diligence to prevent the offence") leaves room for interpretation and might not provide clear criteria for determining liability. The broad wording might encompass a wide range of roles and positions, potentially including individuals who had not real influence or control over the company's actions and decisions.<br><br>Liability on employees, whether civil or criminal, reduces Bangladesh's competitiveness globally and creates an unfavourable environment for foreign direct investment. Further, criminal liability is grossly disproportionate and creates the wrong incentives for intermediary service providers that may lead to over-blocking due to the need to avoid harsh sanctions on employees. |
| 37<br>**The service provider not to be responsible.—** No service provider shall be liable under this Act or rules made thereunder for facilitating access to any data- information, if he proves that the offence or | We request clarity that the service providers will not be liable for any user-generated content, and will not be deemed to have abetted or aided in the transmission or broadcasting of such content, by merely enabling content to be created, transmitted, broadcasted, or hosted on its platform.<br><br>We request clarity that liability may arise only if the intermediary, after receiving a duly reasoned takedown |

| Section | Recommendations |
|---|---|
| breach was committed without his knowledge or he tried his best to prevent the offence. | request from a competent authority formally putting them on notice of unlawful content on the platform, unreasonably fails to action the content.<br>We recommend introducing a Good Samaritan provision barring lawsuits for actions taken in good faith or in a diligent manner.<br><br>As currently drafted, this safe harbour provision does not afford adequate protection to intermediaries for user-generated content. It requires the service provider to demonstrate that the offence was committed without its knowledge, or that all actions were taken to prevent it. Basically, it reverses the burden of proof and presumption of innocence.<br><br>Use of phrases like "direct involvement" and "tried his best to prevent the offence " (or "exercised all due diligence to prevent the offence") leaves room for interpretation and might not provide clear criteria for determining liability. It could lead to disputes over the level of effort or diligence required. Without a robust safe harbour framework, intermediaries are likely to be either (i) dis-incentivised from operating in the Bangladeshi market out of concerns about the risk of liability, or (ii) prone to be over-aggressive in removing content, potentially by employing pre-publication filters, which (as explained above) is inconsistent with the fundamental right of freedom of speech protected by the Bangladesh constitution and international human rights instruments. Either way, the lack of safe harbour provision harms both users and the intermediaries operating services that benefit users. |
| **Lack of proper procedural safeguards** | |
| **CHAPTER III, 8 (1) & 8 (2)**<br>(1) If any data- information related to any matter under the jurisdiction of the Director General, being published or propagated in digital or electronic media, creates threat to cyber security, the Director General may request the Bangladesh Telecommunications and | While the provision requires the Director General to communicate complaints to the BTRC, the language is open-ended and ambiguous, as it does not expressly state that (a) the BTRC is the sole authority for content-related matters, and (b) other government agencies will also have to communicate through BTRC.<br><br>A currently drafted, it runs contrary to the recommendations made in the UN Special Rapporteur Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/38/35 2018), which notes" |

| Section | Recommendations |
|---|---|
| Regulatory Commission, hereinafter referred to as BTRC in this section, to remove or, as the case may be, block the such data-information.<br>(2) If it appears to the law-and-order enforcing force that any data-information published or propagated in digital media hampers the solidarity, financial activities, security, defence, religious values or public order of the country or any part thereof, or incites racial hostility and hatred, the law-and-order enforcing force may request BTRC to remove or block the data-information through the Director General. | *"States should refrain from adopting models of regulation where government agencies rather than judicial authorities, become the arbiters of lawful expression"* Such a system is likely to have a negative effect on speech and expression, and is inconsistent with global best practices.<br><br>We recommend including express provisions requiring due process to be followed before issuance of a takedown request (TDR).<br><br>Requiring TDRs to take the form of duly-reasoned court orders is consistent with Bangladeshi law, which requires that orders be well-reasoned and written in order to be valid and enforceable. Such a duly processed TDR advances transparency goals, as it ensures that intermediaries are aware of why content is prohibited / being restricted. This will facilitate compliance by intermediaries, by making it easier and faster for them to review and assess TDRs, and to action them where appropriate.<br><br>The BTRC, as the sole authority in issuing takedown requests should, at minimum:<br>- Clearly identify the content (with reference to the URLs or other information that will help sufficiently identify the content);<br>- Clearly designate the content as unlawful with specific reference t the provision of the applicable law that it violates;<br>- Provide sufficiently detailed explanation of the factual and legal basis of the finding of unlawfulness and why the content should be removed or ceased to be hosted or disabled from/on the platform;<br>- We recommend providing reasons demonstrating that the removals is necessary, proportionate and reasonable restrictions;<br>- We request ETDA to certify that the request is submitted in good faith and that the information and allegations contained therein are accruable and complete. |

As responsible stakeholders, we appreciate the ability to participate in this discussion and the opportunity to provide further inputs into the policy-making process in Bangladesh. **As such,**

**we would like to respectfully request the Government of the Bangladesh to strongly consider these recommendations.**

**We hope that through further engagement on the Draft Regulation, we can work toward preserving the conducive cybersecurity and business environment within Bangladeshi's digital economy ecosystem.**

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact us directly at Secretariat@aicasia.org or +65 8739 1490. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions.

Thank you for your time and consideration and we look forward to hearing from you.

Sincerely,

**Jeff Paine**
**Managing Director**
**Asia Internet Coalition (AIC)**