

Comments by BLAST on the Cyber Safety Act, 2023 (Draft)

Summary

1. This submission on the draft ‘Cyber Safety Act’ (CSA) has been prepared by the Bangladesh Legal Aid and Services Trust after review of the draft posted on the website of the Information and Communication Technology Division of the Ministry of Posts and Telecommunications and Information Technology.
2. BLAST welcomes the decision to repeal the DSA, and the recognition that this is required to address the concerns widely raised over its use over the years of its operation. It welcomes the proposals to reduce sentences provided for some offences, to make some offences are made bailable, and to do away with imprisonment as a punishment for the offence of defamation.
3. However, BLAST is concerned that the proposed law does not bring in significant changes to the definitions of offences contained in the DSA, or to applicable procedures. As such it does not effectively ensure legal protection for victims of cyber offences, such as women, children or members of marginalized communities, or provide sufficient safeguards to persons who are arrested or accused of committing offences. Its key concerns are set out below.

Key Concerns

1. The provisions of the Draft Act conflict with its stated intent and Preamble

Several provisions of the Draft Act retain provisions (Sections 8, 21, 25, 28, 29, 31, 32, 43, and 53) on restraint of speech and freedom of expression, contrary to the express intent of the law set out in the Preamble. The Preamble to the Draft Act states that it is being enacted to ensure cyber security and to ensure the identification, prevention, restraint and prosecution of offences committed through digital or electronic mediums. The ambiguity and over-broad nature of the said provisions, is an unreasonable incursion on the right to freedom of expression.

Certain terms in the Draft Act suffer from ambiguity and overbreadth

The terms in certain provisions (for example, Sections 21 and 28) are overbroad and vague, for example:

Section 21 criminalizes any speech which is considered to amount to “propaganda or campaign”. These terms are ambiguous and overbroad. The terms “propaganda” or “campaign” are unclear and vague.

Section 28 criminalizes any publication which may hurt or incite religious sentiments. In the absence of any definitions, these terms are highly subjective, and can be weaponized to target minorities.

The criminalization of defamation and similar publication torts as offences under this Act is a severe restriction on the freedom of expression, open to abuse and arbitrary enforcement, and is contrary to the protections guaranteed under the Constitution. This can also exacerbate malicious prosecution of women who may resort to online support groups to voice grievances, abuse or harassment and then subsequently be prosecuted for intentional publication of “attacking information” .

2. Omission of Cybercrimes against women and children

The Draft CSA’s stated aims are to regulate cyber security and to detect, prevent, and prosecute crimes committed through digital or electronic means, but it does not expressly address or define internationally recognised cybercrimes against women, children, and minorities. It does not criminalise the creation, possession or dissemination of material on child sexual abuse. It also does not address the malicious publication or dissemination of ‘revenge pornography’,, or threats of rape or assault against women and children.

3. Conflict between the Children Act and Draft CSA

Section 3 of the Draft CSA provides that it will prevail over others laws, creating a possible conflict with for example, the Children Act, 2013, which sets out special procedures for cases involving children in conflict with the law.

4. Disproportionate sentences

While the Draft CSA has reduced the maximum sentences applicable for some offences, the range of sentences of imprisonment provided are still disproportionately high for speech related offences where there is no direct harm caused to any person. Furthermore, the fines are also disproportionately high for these offences (compared to offences against the person, e.g., grievous hurt, which do not carry such heavy fines under penal laws).

5. Removal or Blocking of Content/ Internet Shutdowns

Section 8 of the Draft Act grants the Director General of the CSA the power to remove or block online content, on overbroad and subjective grounds. This could severely restrict access to information on an arbitrary and discriminatory basis. It could also

disproportionately impact the provision of information and online education for vulnerable groups. This section also grants the Director General wide powers to order internet shutdowns, which could impact a whole host of activities from banking, healthcare, emergency communication and education, and would be a disproportionate response to a “perceived offence”.

6. **Procedural Issues**

- (a) **Arrest:** The draft continues to provide broad powers to law enforcers to arrest without warrant for any offences under the CSA as is the case with the DSA, even if those do not pose a direct threat to any person. It does not provide any specific procedures and guidelines that must be adhered to, ensuring that any actions taken for addressing suspicions of such threats are based on legitimate grounds rather than arbitrary decisions.
- (b) **Investigation:** Under Section 39, the Investigation Officer has unlimited authority to conduct search and seizure. Under Section 40, the Investigating Officer is not required to obtain a warrant in respect of such investigations, seizing or impounding of devices and collection of information.
- (c) The authority to collect traffic-data without further qualification ignores current technology and jurisprudence in many countries where requisition of such data requires specific time-period requirements and similar protections to prevent abuse, harassment and invasion of privacy of citizens.
- (d) **Time period for Investigations:** The Draft also does not provide any specific grounds for when Tribunals can allow continuation of investigations beyond the finite time periods.

Recommendations

In this context, BLAST respectfully submits that the Government take the following measures:

1. Extend the period of consultation on the Draft CSA.
2. Hold public hearings in this regard with all concerned stakeholders, and in particular with women’s groups, development organisations, representatives of marginalised communities, and disabled people’s organisations.
3. Establish a mechanism for review of the reportedly 7000 cases filed under the Digital Security Act from 2018 to date (and those earlier filed under Section 57 of the Information Communication and Technology Act, 2006) to identify cases involving miscarriage of justice and to provide relief and redress to those affected.
4. Review comparative laws, and incorporate best practices including through considering ratification of the Cybercrime Convention and aligning the Draft Act with the provisions of the Convention to comprehensively address the definitions of cyber related offences,

ensuring protection of women, children and other protected groups, including marginalised communities.

5. **Offences:**

(a) Define and address specific cyber crimes against women, children, and minorities.

(b) Remove the vague speech offences under sections 21, 25, 28, 29, and 31 which allow subjective interpretation and arbitrary application, and provide disproportionately heavy penalties. Such offences under DSA have also reportedly affected women, girls, and children.

(c) Ensure children are not implicated under the draft law for any speech offences.

6. **Arrest:** Restrict arrest without warrant to only offences that pose a direct threat to body and personal safety. Provide specific procedures and guidelines that must be adhered to, ensuring that any actions taken for addressing suspicions of such threats are based on legitimate grounds rather than arbitrary decisions.

7. **Investigation:** Provide specific and precisely defined grounds when Tribunals can allow continuation of investigations beyond the finite time periods, ensuring any exceptions are not regularly practised.

8. **Saving Clause:**

(a) Amend the saving clause, explicitly stating that no case for speech offences under DSA should continue, specifically barring continuation of cases against women and children.

(b) Clarify the position of cases under section 57 ICTA after DSA gets repealed.

9. **Remedy against misuse:** Ensure remedy for those wrongly implicated under the law.

10. **Institutional Independence of authorities:**

(a) Establish the independence of the Cyber Security Agency.

(b) Establish independent digital forensic labs separate from the government for ensuring independence and checks and balances.

11. **Forensic experts:** Make examination of digital forensic experts in court mandatory to ensure transparency and credibility of their reports.