TRANSPARENCY INTERNATIONAL BANGLADESH

Social movement against corruption

Digital Security Act 2018 and the draft Cyber Security Act 2023 :

A Comparative Analysis

29 August 2023

Background

Since its inception, the Digital Security Act 2018 (DSA) of Bangladesh has faced extensive criticism for being used as a tool against freedom of expression, media freedom, human rights, and dissension.

- From September 2018 until January 2023, over 7,001 cases have been filed across the country under the DSA for exercising the right to free speech, dissenting voice, and independent media reporting.
- The fate of most of the accused was left uncertain, as only 2 per cent of those accused under the DSA witnessed their cases resolved in court, resulting in being found guilty, declared not guilty, or having the cases dropped.
- Opposition politicians, journalists, businesspeople, students, and private employees were among the main victims of the DSA.
- Ruling party affiliates were the largest group prosecuting journalists.
- On average, a ruling party activist has filed a case every week over the last four years.
- One out of every three individuals facing charges under the DSA has been arrested.
- During these years, 60 per cent of cases were filed for Facebook activity.
- Between January 2020 and February 2022, approximately 2244 individuals faced charges in 890 cases, including 254 politicians and 207 journalists, with the majority of accusers being political party members (206), the Rapid Action Battalion (RAB, 87), and government officials (43)

Background

- Transparency International Bangladesh (TIB) along with several national and international organisations and people at large have consistently called for repealing the DSA due to its potential misuse of free speech.
- In response to the mounting national demands and international critique, on 7 August 2023, the Cabinet of Bangladesh decided to replace the contentious Digital Security Act 2018 (DSA) with the draft Cyber Security Act 2023 (draft CSA).
- The final draft of the CSA was approved on 28 August 2023.

Comparative analysis between DSA and draft CSA

- The draft CSA is essentially a renamed version of the DSA, with only a few alterations in the form of apparently reduced severity of punishments. For example, the draft CSA does not provide for punishments for committing an offence a second time in some instances.
- In certain sections, the draft CSA provides shorter imprisonment sentences compared to the DSA, though it proposes higher fines than the DSA in several sections.
- The time allowed to complete the investigation under the draft CSA as per section 39 (DSA 40) has been extended to 90 days instead of 60.
- The draft CSA has more non-cognisable and bailable sections than the DSA.
- In substance, the draft CSA contains all the provisions from the DSA that compromise freedom of speech, dissent, thought and conscience, freedom of the press, and independent journalism.

Evaluation of the Draft Cyber Security Act

- The provisions outlined in sections 8, 9, 10, and 11 of the draft Cyber Security Act pertain to preventive measures and capabilities such as data removal or blocking, emergency response, digital forensic labs, and quality control.
- Data Removal or Blocking (Section 8): The Act's provisions enable the removal or blocking of data information that poses a threat to digital security or public order. While such provisions could be essential in addressing immediate threats, the criteria and oversight mechanisms for determining what constitutes a threat should be well-defined to avoid potential misuse. Additionally, ensuring transparency in the decision-making process and mechanisms for appeal are important to prevent censorship.
- This section at its current form raises concerns regarding its potential misuse, vagueness of terms, and potential impacts on freedom of expression.
- *ICCPR and International Standards:*
- The ICCPR emphasises that any interference with individuals' privacy rights, including data removal or blocking, must adhere to principles of legality, necessity, proportionality, and due process. These principles are aimed at ensuring that any action taken by authorities respects individual rights while maintaining the legitimate aims of cyber security.

Evaluation of the Draft Cyber Security Act

- *Vagueness and Potential Misuse:*
- The language used in this section contains vague terms such as "threat to digital security," "solidarity," "financial activities," and "religious values." The lack of clear definitions for these terms creates ambiguity and a risk of broad interpretation by authorities. Such vagueness can lead to arbitrary decision-making and potential misuse of these provisions for suppressing legitimate online expression. The absence of objective standards for determining whether content actually poses a threat or hampers solidarity undermines the predictability required under international human rights law.

Offence and Punishment

- **Overbroad Restrictions on Expression:** The Act includes provisions that criminalise the publication or transmission of offensive, false, or threatening data information (Section 25) and content that hurts religious values or sentiments (Section 28). While curbing harmful content is important, these provisions must be carefully crafted to avoid vague terms that could lead to overbroad restrictions on freedom of expression. International human rights law, including the International Covenant on Civil and Political Rights (ICCPR), emphasises that restrictions on expression must be narrowly defined and proportionate to a legitimate aim.
- **Criminalisation of Online Activities:** Some provisions criminalise actions that might not warrant severe criminal penalties, such as illegal access to computers, computer systems, or networks (Sections 17 and 18). Best practices suggest that penalties should be commensurate with the gravity of the offence and should not disproportionately restrict individual rights. Excessive criminalisation can have a chilling effect on legitimate online activities.

Offence and Punishment

- **Violation of Right to Privacy:** The Act addresses identity fraud or personation (Section 24) and unauthorised collection or use of identity information (Section 26). While the protection of identity information is important, these provisions should be analysed in light of the right to privacy. The collection and use of personal data should adhere to established data protection principles, and the Act should ensure that lawful authority is defined clearly to prevent abuse.
- **Potential for Overreach and Disproportionate Punishments:** Some provisions, such as those related to cyber terrorism (Section 27) and hacking (Section 33), propose severe punishments, including 14 (fourteen) years imprisonment and hefty fines. Such penalties could deter cybersecurity professionals from conducting legitimate research or reporting vulnerabilities, hindering the overall security of digital systems.

Investigation of Offence and Trial

- **1. Investigation and Powers (Sections 38-42):** The Act grants certain powers to the Investigation Officer for the investigation of cybercrimes, such as search and seizure of digital devices, data, and materials related to offences. While these powers are necessary for effective investigation, it's important to ensure that they are exercised with proper oversight and accountability to prevent misuse. The procedures for obtaining search warrants and conducting searches must be clearly defined, and there should be safeguards against potential abuse.
- **Lack of Technical Expertise:** Cybercrimes involve intricate digital mechanisms, data breaches, and sophisticated online activities that require a deep understanding of digital forensics and cyber techniques. Traditional police officers might not possess the technical proficiency needed to investigate and gather evidence in the digital realm effectively.

Investigation of Offence and Trial

- **Complex Investigations:** Cybercrimes often transcend geographical boundaries and involve multiple layers of virtual communication. Effective investigation in such cases requires collaboration with international law enforcement agencies, cyber security experts, and digital forensics specialists who can navigate the complexities of digital footprints.
- Sections 40, 45, and 46 confer the police investigator with overly broad powers that risk being misused and abused. The absence of an independent judicial oversight mechanism for the process of seizing computers and personal property adds to this concern. These provisions lack clear standards and can be invoked under the vague criterion of "investigation," which lacks a precise definition.

Cyber Security

- The provisions outlined in sections 5, 6, and 7 of the draft Cyber Security Act pertain to the establishment, structure, and appointment of key personnel within the Cyber Security Agency. While these provisions are a step in the right direction towards establishing an agency responsible for cyber security in Bangladesh, a comprehensive analysis reveals areas that could benefit from further refinement and alignment with global best practices.
- **Establishment of Agency (Section 5):** The establishment of a dedicated agency for cyber security is crucial for addressing evolving cyber threats. However, the scope and functions of the agency should be more explicitly defined within the Act itself. Additionally, the Act should lay out the agency's responsibilities, such as incident response, threat intelligence, and coordination with other relevant authorities, to ensure a comprehensive cyber security framework.
- **Appointment and Expertise (Section 6):** The requirement for appointing the Director General and Directors with expertise in computer or cyber security is a positive step. However, the Act should further emphasise the importance of multidisciplinary expertise, including legal, technical, and policy skills. This ensures that the agency is equipped to tackle the diverse challenges of cyber security effectively.
- **Manpower and Resources (Section 7):** While the provision allows the agency to appoint necessary employees, it lacks specificity regarding the types of roles required, such as cybersecurity analysts, incident responders, legal experts, and policy advisors. The Act could include a broader framework for the agency's organisational structure and required skill sets.

National Cyber Security Council

- The provisions outlined in sections 12 - 14 establish the National Cyber Security Council, comprising various government officials and specialists, to oversee the implementation of the draft Cyber Security Act, which is a positive step towards enhancing cyber security efforts. However, certain aspects of the composition and authority of the Council warrant consideration in terms of the best practices for effective governance in the realm of cyber security.
- **Expertise and Representation:** While the draft Act's Council includes officials from key government bodies, such as the Ministry of Post, Telecommunication and Information Technology, the Ministry of Law, Justice and Parliamentary Affairs, and others, the expertise in cyber security might be better addressed with dedicated representatives from specialised entities. For example, the armed forces, intelligence agencies, and police chiefs may not possess the technical knowledge required to address cyber security challenges effectively.
- **Authority and Independence:** The Council's role is substantial, including providing directions, advice and formulating policies for digital security. To ensure the Council's effectiveness, it should be granted sufficient authority and independence in decision-making while also being subject to appropriate oversight mechanisms.

Critical Information Infrastructure

- The provision of Critical Information Infrastructure (CII) in the draft Cyber Security Act (Section 15 – 16) is a crucial component for safeguarding essential digital assets. However, while the provision recognises the significance of monitoring, inspection, and expertise, it falls short of fully addressing the comprehensive tech and human solutions that are expected in a robust cyber security law.
- To enhance the tech and human solutions within the provision of Critical Information Infrastructure, the draft Cyber Security Act could have incorporated requirements for mandatory cybersecurity measures, incident response plans, and adherence to technical standards. Additionally, the law could outline the establishment of specialized cybersecurity teams and emphasise training and skill development for personnel involved in protecting critical assets.

Concluding Remarks

- Some recent incidents underscore a glaring discrepancy between the aspirations of digital security measures and the reality of their implementation. Despite the existence of the Digital Security Act (DSA), the National Computer Incident Response Team (N-CIRT), the National ICT Policy and Cyber Security Strategy, a series of cyber-attacks, data leaks, and breaches have revealed the limitations of the current legal and technical framework in safeguarding digital assets and personal information.
- The incidents involving Biman Bangladesh Airlines, government institutions, and the leakage of sensitive personal data from the Office of the Registrar General, Birth & Death Registration highlight the vulnerabilities that persist even under the existing security measures.

- The approval of the draft Cyber Security Act (draft CSA) with provisions similar to the DSA, despite the ongoing challenges, raises strategic questions about the direction of the nation's cybersecurity approach. The fact that the same provisions persist in the draft CSA suggests a continuity of approach that has not yielded the desired results thus far.
- The risk here is twofold:
  - first, it could perpetuate the existing gaps and vulnerabilities that threat actors exploit, and
  - second, it would continue to stifle the space for online freedom of expression due to the potential misuse of the repressive provisions, as evidenced by numerous cases filed under the DSA.

Concluding Remarks

- To navigate this complex landscape, a strategic shift is needed. This entails not just enacting legal frameworks but also aligning them with evolving cyber security threats and international human rights standards.
- A strategic approach should include provisions that prioritise proportionality, accountability, and judicial oversight while fostering collaboration between government agencies, private sector entities, and cyber security experts. Moreover, investing in cyber security education and workforce development is vital to bridge the technical gap and mitigate potential risks.

Thank You