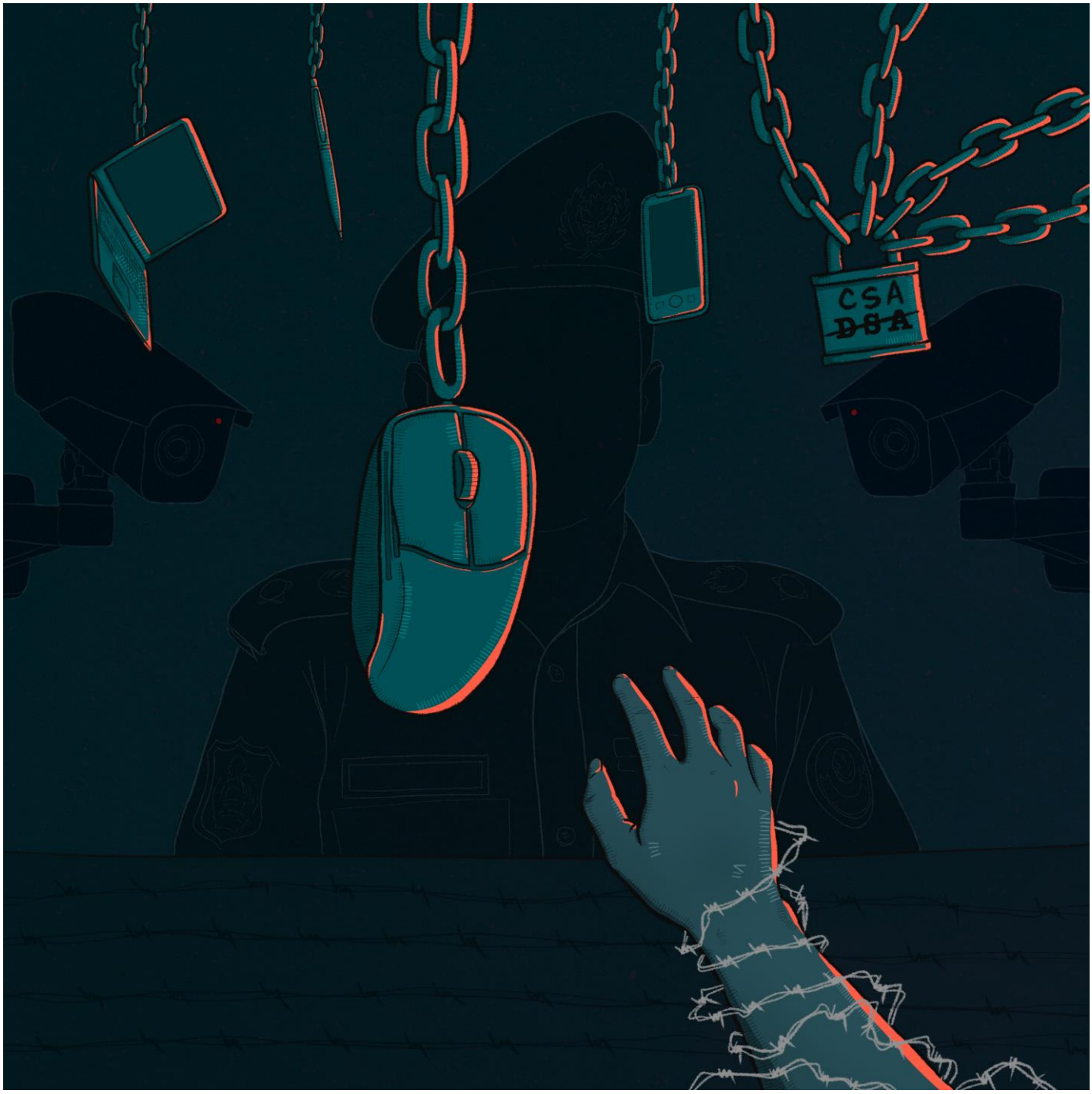
Flygtningenævnets baggrundsmateriale

Bilagsnr.:	**500**
Land:	Bangladesh
Kilde:	Amnesty International
Titel:	Repackaging Repression The Cyber security act and the continuing lawfare against dissent in Bangladesh
Udgivet:	1. August 2024
Optaget på baggrundsmaterialet:	10. oktober 2024



REPACKAGING REPRESSION

THE CYBER SECURITY ACT AND THE CONTINUING LAWFARE AGAINST DISSENT IN BANGLADESH

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

© Amnesty International 2024
Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode
For more information please visit the permissions page on our website: www.amnesty.org
Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.
First published in 2024
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: ASA 13/8332/2024
Original language: English

amnesty.org

Cover photo: *An illustration of a hand reaching out and wrapped in barbed wire in the foreground while a mobile phone, laptop, pen and mouse hang in the background, all chained to a piece of lock labelled 'CSA' with 'DSA' struck out. © Ema Anis/Amnesty International*

AMNESTY INTERNATIONAL

CONTENTS

1. EXECUTIVE SUMMARY

> **"The government wields full power to decide what can and cannot be said in the cyber world, with utmost control but not the least bit of accountability or transparency."**
>
> A Bangladeshi lawyer to Amnesty International

OVERVIEW

The Cyber Security Act 2023 (CSA) is the latest in a series of successive legislation that has repeatedly facilitated the state's ongoing crackdown on peaceful dissent and the right to freedom of expression in Bangladesh. The stated aim of the CSA is to ensure cyber security and criminalise offences which are committed through digital or electronics means. It replaces the controversial Digital Security Act 2018 (DSA) which had been enacted in 2018 with the same purported objective but had instead been used as an instrument of harassment by the ruling party and its affiliates to stifle peaceful dissent. Similarly, the DSA had repealed and replaced an earlier controversial provision, namely Section 57 of the Information and Communications Technology (ICT) Act 2006, which criminalised the publication of 'fake, obscene, or defamatory information' in electronic form and was systematically used to gag dissent. The successive enactment of these repressive laws has been accompanied by the misuse of the criminal justice system to target and prosecute those peacefully exercising their right to freedom of expression. This epitomises the lawfare (i.e. legal warfare) that the government of Bangladesh has launched against dissent in the past decade, especially targeting journalists, human rights defenders, activists, critics and dissidents.

Amnesty International is concerned that the CSA repackages almost all repressive features of the DSA (and Section 57 of the ICT Act that preceded it) and marks a continuation of the state's clampdown on civic space and human rights, particularly the right to freedom of expression in Bangladesh. This briefing primarily draws on legislative analysis of the CSA and DSA and 20 interviews conducted with a range of stakeholders, including former detainees, their relatives, their lawyers as well as journalists and human rights defenders in Bangladesh. This briefing argues that although the government of Bangladesh has presented the CSA as a major reform, it is essentially the same piece of legislation as the DSA, with some minor amendments. In June 2022, the Office of the United Nations High Commissioner for Human Rights (OHCHR) issued a technical note to the Government of Bangladesh providing nine specific recommendations on reforming the DSA to bring it in conformity with international human rights law. Amnesty International's analysis shows that the Government of Bangladesh has only implemented one of the nine recommendations of the OHCHR in the CSA; it has partially implemented three recommendations, while the remaining five recommendations have been completely ignored in the CSA. Further, Amnesty International's legislative analysis has found that the CSA retains 58 of the 62 provisions of the DSA: 28 provisions are retained verbatim; 25 provisions are retained with minor changes (such as related to sentencing or terminological alterations) and five provisions are retained with some procedural amendments. The CSA only introduces one new provision, which is an offence for filing false cases. Therefore, 58 of the 59 provisions in the CSA were inherited from the DSA, either verbatim or with minor changes or procedural alterations. Amnesty International's legislative analysis also found that the government made changes to 16 sections in the final version of the CSA enacted in September

2023, compared to the draft version which was published for public feedback in August 2023. Only two of these changes were substantive, while the remaining changes were minor terminological or procedural alterations. Therefore, Amnesty International believes that the call for feedback on the CSA draft was a mere tick box exercise, as substantial recommendations made by civil society were completely ignored.

AUTHORITARIAN SPEECH OFFENCES

Amnesty International is also concerned that the CSA retains the five authoritarian speech offences from the DSA which have repeatedly been used by the ruling party and its affiliates to muzzle peaceful dissent. The five speech offences include: 'propaganda against the spirit of liberation war' (Section 21), 'false and offensive information' (Section 25), 'hurting religious sentiments' (Section 28), 'defamatory information' (Section 29), or 'deteriorating law and order' by 'disrupting communal harmony' (Section 31). Amnesty International's analysis has found these provisions fail to meet the requirements of legality, necessity, and proportionality under international human rights law. They penalise the legitimate expression of opinions or thoughts and violate Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which guarantees the right of everyone to freedom of expression including the right to hold opinions without interference.

SWEEPING POWERS OF ARREST, SEARCH AND SEIZURE

Amnesty International welcomes the reduction in the number of cognisable and non-bailable offences in CSA in comparison to the DSA. However, the CSA retains the sweeping powers of arrest, search and seizure given to law enforcement agencies under the DSA. Section 42 of the CSA is identical to Section 43 of the DSA and continues to authorise any police officer to search premises, seize computers and similar hardware, and search the body of a person and arrest individuals – without a warrant from the court. The unfettered discretion granted to police under Section 42 of the CSA (like Section 43 of the DSA before it) inherently risks misuse and abuses of power. Therefore, despite the progressive conversion of previously cognizable offences under the DSA to non-cognizable offences, the police may always resort to the broadly worded powers under Section 43 to make arrests without warrants where it pleases.

Amnesty International has found that in spite of the sweeping powers given to law enforcement agencies to search and seize devices under the CSA, there are no clear safeguards in Bangladeshi law regarding how the authorities should use and store the data in seized computers and similar hardware. UN Resolution 68/167 warns against the capacity of governments to undertake surveillance, interception, and data collection, which may violate or abuse human rights, particularly the right to privacy guaranteed under Article 17 of the ICCPR. There must be clear regulation on how such data will be handled or destroyed at the conclusion of an investigation or trial. The law should also clarify how the seized computer or hardware will be returned to its owner. Regrettably, the legal framework in Bangladesh fails to provide these safeguards, thereby threatening the rights to privacy and a fair trial of those accused of committing cyber offences under the CSA, DSA and ICT Act.

ARBITRARY POWER TO REMOVE OR BLOCK DATA

The CSA also continues to empower government authorities to arbitrarily block or remove data. Under Section 8 of the CSA, the Cyber Security Agency (which is controlled by the government) and law enforcement agencies can request the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block information and data from the internet on broad grounds. Not only are the grounds stipulated in Section 8 vague, they also empower the Cyber Security Agency and law enforcement agencies to make blanket requests to the BTRC to remove and block information and data based on nothing more than their own assessment of a situation. Their decision alone is sufficient to block websites or other digital means of sharing information and data, without any judicial oversight or opportunity to appeal the process. Although rhetorically termed a 'request' to remove or block data, Section 8(3) makes it clear that any such request from the Cyber Security Agency or law enforcement forces is binding on the BTRC since it 'shall' 'instantly remove' or 'block the data'. Allowing a government-controlled agency and law enforcement agencies the power to essentially force a regulatory body to remove or block data nullifies the latter's independence, granted by statute.

CASES UNDER THE CSA

Journalists and human rights defenders who spoke to Amnesty International cautioned that it has become more difficult to document cases under the CSA. As most offences under the CSA, including the five authoritarian speech offences, are now non-cognisable offences, they have to be filed directly before courts as opposed to police stations, where access is far more limited. Despite the official data gap and likelihood of underreporting, Amnesty International found media reports of at least ten instances where CSA cases have been filed against individuals for allegedly defaming the prime minister or other high ranking government officials on social media. Additionally, Amnesty International has investigated and analysed three cases under the CSA which show that it is being used to curb freedom of expression in the same way as the DSA. These three cases pertain to: an atheist blogger who remains in jail for charges related to hurting 'religious values or sentiments' and deteriorating law and order despite being granted bail; a climate activist and graphic designer who was jailed after he designed posters critical of his local mayor and his devices remain seized by the police; and a religious preacher who has been prosecuted for posting a video on social media which was accused of hurting 'religious sentiments'.

A STATE OF SELF-CENSORSHIP

> **"From the most senior journalist to a small fry Youtuber, everyone is now in a state of self-censorship because no one, and I mean no one, can afford to pay the price of speaking up."**
>
> A news editor to Amnesty International

The state's persistent lawfare against dissent in the past decade using the DSA and Section 57 of the ICT Act has bulldozed journalists, activists, human rights defenders, and critics into a state of self-censorship which will continue to exist unless the repressive features retained in CSA are removed. All journalists and human rights defenders interviewed by Amnesty International described a culture of fear that has been catalysed by relentless prosecution of speech offences under the DSA and the ICT Act followed by the enactment of the CSA which retains most of the repressive provisions of the former laws. Additionally, lawyers, and defendants who Amnesty International spoke to emphasised that scores of cases that were filed under the now repealed DSA and Section 57 of the ICT Act remain ongoing, due to the protracted trial process in Bangladesh. The DSA allowed cases filed under Section 57 of the ICT Act to continue if they were pending at any stage of trial. The repeal and savings clause in the CSA is even broader since it allows any and all cases filed under DSA to continue even if the investigation or trial process has not commenced. As such, the state has been able to continue framing charges under the DSA against individuals as recently as April 2024, seven months after the repeal of the DSA. As one defendant in an ICT Act case explained:

"On the one hand the state says the ICT Act and DSA are gone, but on the other hand they are not sparing anyone against whom a case had been filed under these laws. For us, these laws never ceased to exist, and their draconian provisions continue to plague our lives. We continue to face the full brunt of state-sanctioned legal harassment."

CONCLUSION AND KEY RECOMMENDATIONS

A narrow focus on the repeal of a singular legislation, such as the DSA, renders limited benefit especially given the growing repression in Bangladesh. This narrow focus has allowed Bangladesh authorities to diffuse mounting international pressure by undertaking performative reform which simply repackages repressive provisions in a new law. Therefore, international advocacy efforts should adopt a broader focus that goes beyond challenging a singular piece of legislation to confronting the wider crackdown on civic space including through the repressive penal practices and procedures which the state has at its

disposal. These include the police's power to arrest and search individuals without warrants, pretrial detention through refusal of bail and legal persecution in the name of prosecution.

In light of the analysis, Amnesty International calls on the Government of Bangladesh to:

- repeal or review and amend all laws that violate human rights, including the rights to freedom of expression, privacy and liberty, in particular: sections 8, 21, 25, 28, 29, 31 and 43 of the CSA to fully comply with international human rights law, including the ICCPR, to which Bangladesh is a state party.
- amend provisions which allow overbroad powers of arrest, search, and seizure, including Section 42 of the CSA so such powers are clearly and narrowly defined. All investigative powers under the law must be subject to safeguards and judicial oversight in line with international human rights law.
- immediately and unconditionally release all those detained under the ICT Act, DSA, CSA or any other law solely for peacefully exercising their human rights.
- introduce legislation expressly granting anyone who has been the victim of unlawful arrest or detention to have an enforceable right to effective remedies, including adequate compensation as stipulated in Article 9(5) of the ICCPR.
- ratify the First Optional Protocol to the ICCPR to enable individuals to submit complaints to the Human Rights Committee of violations of their rights set out in the Covenant
- extend an invitation to the UN Special Rapporteur on the rights to freedom of opinion and expression to carry out a fact-finding visit to Bangladesh.

2. BACKGROUND

The Cyber Security Act 2023 (CSA) is the latest in a series of successive legislation that has repeatedly facilitated the state's ongoing crackdown on human rights including the right to freedom of expression in Bangladesh. The right to freedom of expression is guaranteed under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), to which Bangladesh has been a state party since 2000. Article 19 of the ICCPR guarantees the right of everyone to freedom of expression including the right to 'hold opinions without interference'. Similarly, Article 39 of Bangladesh's Constitution guarantees 'freedom of thought and conscience', 'the right of every citizen to freedom of speech and expression' and 'freedom of the press' by encompassing these within the right to freedom of thought and conscience, and of expression.

The CSA replaces the controversial Digital Security Act 2018 (DSA) which had been used as an instrument of harassment by the ruling party and its affiliates to stifle peaceful dissent since its enactment in 2018. Similarly, the DSA had been enacted to repeal and replace an earlier controversial provision that was also systematically used to gag dissent, namely Section 57 of the Information and Communications Technology (ICT) Act 2006, which criminalised the publication of 'fake, obscene or defamatory information' in electronic form.[1] In 2013, the ICT Act was amended to make offences under Section 57 non-bailable while also allowing the police to make arrests without warrants.[2] Despite the government's assurances to uphold the right to freedom of expression at the time, the DSA rehashed Section 57 of the ICT Act into four new authoritarian offences. These were: Section 25(a) (publication of offensive, false or threatening information in order to annoy, insult, humiliate or malign a person), Section 25 (b) (publishing propaganda or false information with an intention to affect the image or reputation of the country or to spread confusion), Section 28 (hurting religious sentiments) and 31 (publishing anything which destroys communal harmony or deteriorates the law-and-order situation). The DSA also introduced another sweeping offence under Section 21 which criminalised 'propaganda or campaign' against 'the spirit of liberation war', and 'the father of the nation, national anthem and national flag'. These five authoritarian offences under the DSA were repeatedly used against dissidents to set the parameters of acceptable speech and swiftly penalised even the slightest forms of dissent.[3] Amnesty International believes that these five overly broad offences are designed to penalise legitimate expression of opinions or thoughts critical of the government or its officials. Currently, the CSA retains most of the repressive features of the DSA, including these five offences.

Amnesty International has long documented the assault on the right to freedom of expression in Bangladesh, including under Section 57 of the ICT Act and the DSA, and has repeatedly called for the Bangladesh government to uphold its international human rights obligations including to respect, protect, promote and fulfil the right to freedom of expression.[4] While there are certain other laws which also impermissibly restrict the right to freedom of expression (such as the Bangladesh

[1] Amnesty International, *Caught between fear and repression: Attacks on freedom of expression in Bangladesh* (2017) (Index: ASA 13/6114/2017), p. 50. https://www.amnesty.org/en/documents/asa13/6114/2017/en/; Article 19, *Bangladesh: Information Communication Technology Act* (2016) https://www.article19.org/resources/bangladesh-information-communication-technology-act/

[2] International Commission of Jurists (ICJ), *Briefing Paper on the amendments to the Bangladesh Information Communication Technology Act 2006* (2013), https://www.icj.org/wp-content/uploads/2013/11/ICT-Brief-Final-Draft-20-November-2013.pdf

[3] Amnesty International, *No Space for Dissent – Bangladesh's Crackdown on Freedom of Expression Online* (2021) (Index: ASA 13/4294/2021), http://www.amnesty.org/en/documents/asa13/4294/2021/en/

[4] See for example: Amnesty International, *Caught between Fear and Repression* (previously cited); Amnesty International, *Bangladesh: Muzzling Dissent Online* (2018) (Index: ASA 13/9364/2018), https://www.amnesty.org/en/documents/asa13/9364/2018/en/; Amnesty International, *No Space for Dissent* (previously cited); For a list of all publications by Amnesty International on freedom of expression in Bangladesh, see: https://www.amnesty.org/en/search/bangladesh/?qlocation=1723&qtopic=2094

Telecommunication Act 2001 and Pornography Control Act 2012),[5] the ICT Act and the DSA had been most frequently used to stifle peaceful dissent and undermine freedom of press for the past decade. Ahead of the repeal of Section 57 of the ICT Act, 1,271 people were reported to have been charged under it between 2013 and April 2018,[6] while over 7,000 people were reported to have been charged under the DSA since its enactment in October 2018 till January 2023.[7] The repressive section 57 of the ICT Act was repackaged as the draconian provisions of DSA, which in turn have now been repackaged in the newly enacted CSA. Due to the lack of publicly available official data on criminal justice in Bangladesh, it remains difficult to estimate the frequency with which the CSA has been used so far.[8]

2.1 INTERNATIONAL PRESSURE TO REPEAL THE DSA

Bangladeshi authorities' decision to repeal the DSA came as a result of mounting pressure at national and international fronts.[9] In March 2021, the then UN High Commissioner for Human Rights Michelle Bachelet urged Bangladeshi authorities to urgently 'suspend the application of the Digital Security Act and conduct a review of its provisions to bring them in line with the requirements of international human rights law'.[10] This call came in response to the custodial death of writer Mushtaq Ahmed, who was charged under the DSA for criticising the government's response to the COVID-19 pandemic and suffered nine months of pretrial detention after his bail applications were denied six times.[11] In March 2023, the current UN High Commissioner for Human Rights Volker Türk reiterated the call for the immediate suspension of the DSA pending comprehensive reform to bring it in line with international human rights law.[12] This call came in response to Prime Minister Sheikh Hasina labelling Prothom Alo – the country's largest daily newspaper – 'an enemy of the Awami League, democracy, and the people of Bangladesh' in Parliament.[13] Hours later, a group of individuals barged into Prothom Alo's office in the capital, Dhaka, issued threats and vandalised its logo.[14]

The clampdown on Prothom Alo was in reaction to an article journalist Shamsuzzaman Shams, published by the media outlet on 26 March, the country's Independence Day, covering the cost of living in Bangladesh. Three days after publication, Shams was arbitrarily arrested and detained under the DSA for publishing 'defamatory, false, and fabricated information'. A family member of Shams told Amnesty International, "We were worried sick. There was no warrant issued against him. No one informed us of anything. Even when it was confirmed that he was in custody, that too we came to know from mass media."[15] Shams was initially denied bail and jailed. Although he was later released on bail after spending five days in prison, he continues to face prosecution and if convicted he could face up to seven years imprisonment.

The UN human rights chief's call for the suspension of the DSA came as part of ongoing bilateral discussions between the Office of the High Commissioner for Human Rights (OHCHR) and the government to reform the DSA in line with Bangladesh's obligations under international human rights law. As part of these efforts, in June 2022, the OHCHR published a technical note addressed to the Government of Bangladesh with nine recommendations pertaining to the reform of ten specific sections

---

[5] These include: Official Secrets Act 1925; Bangladesh Telecommunication Act 2001; Pornography Control Act 2012; and Children Act 2013. For a discussion of these restrictions, see: Taqbir Huda, *Promote Digital Citizenship Among Youth in Bangladesh to Accelerate Freedom of Expression'*, Dnet and Friedrich Naumann Foundation for Freedom (2022), p. 4.

[6] Human Rights Watch, *No Place for Criticism Bangladesh Crackdown on Social Media Commentary* (2018), https://www.hrw.org/report/2018/05/10/no-place-criticism/bangladesh-crackdown-social-media-commentary

[7] Dhaka Tribune, "Law minister: Over 7,000 cases under DSA", 05 June 2023. https://www.dhakatribune.com/bangladesh/284852/law-minister-over-7-000-cases-under-dsa

[8] See Section 7 of this briefing.

[9] New Age, "Protests against DSA mounting", 3 April 2023, https://www.newagebd.net/article/198446/protests-against-dsa-mounting; The Daily Star, "Journalists form human chain to demand repeal of DSA", 14 July 2023, https://www.thedailystar.net/news/bangladesh/crime-justice/news/journalists-form-human-chain-demand-repeal-dsa-3368776

[10] Office of the High Commissioner of Human Rights, "Bangladesh: Bachelet urges review of Digital Security Act following death in custody of writer", 01 March 2021, https://www.ohchr.org/en/2021/03/bangladesh-bachelet-urges-review-digital-security-act-following-death-custody-writer

[11] Amnesty International, "Bangladesh: Cartoonist tortured, writer dies in jail", 8 March 2021, https://www.amnesty.org/en/documents/asa13/3800/2021/en/

[12] Office of the High Commissioner of Human Rights, Bangladesh: Türk urges immediate suspension of Digital Security Act as media crackdown continues, 31 March 2023, https://www.ohchr.org/en/press-releases/2023/03/bangladesh-turk-urges-immediate-suspension-digital-security-act-media

[13] 'The Daily Star, *P*rothom Alo is the enemy of AL, democracy, country's people: PM', 10 April 2023', https://www.thedailystar.net/news/bangladesh/news/prothom-alo-the-enemy-al-democracy-countrys-people-pm-3293596

[14] New Age, "Youths breach security, intrude on Prothom Alo office", 11 April 2023, https://www.newagebd.net/article/199148/youths-breach-security-intrude-on-prothom-alo-office

[15] Amnesty International, Bangladesh: Increasing intimidation and harassment of Prothom Alo signals deepening crisis of press freedom in the country (2023), 12 April 2023, https://www.amnesty.org/en/latest/news/2023/04/bangladesh-increasing-intimidation-and-harassment-of-prothom-alo-signals-deepening-crisis-of-press-freedom-in-the-country/

of the DSA to bring it in conformity with international human rights law.[16] All nine recommendations propounded by the OHCHR corresponded to those made by Amnesty International in its analysis of the DSA published in November 2018, a month after the law was enacted.[17]

When the Government of Bangladesh announced the introduction of the CSA to replace the DSA, Amnesty International welcomed the government's decision to repeal the DSA but cautioned that the new law must not replicate the DSA's repressive features.[18] On 9 August 2023, a draft of the Cyber Security Act was published on the website of the Information and Communication Technology (ICT) Division of the Government of Bangladesh, seeking feedback from stakeholders within 22 August 2023.[19] On 22 August 2023, Amnesty International submitted detailed feedback on the draft CSA in an open letter to the Government of Bangladesh.[20] It cautioned that the draft law retains all but one of the offences contained in the DSA verbatim and the only notable changes in the CSA were related to sentencing. It made several recommendations to the government to ensure the right to freedom of expression is protected in line with its obligations under international human rights law.

According to media reports, around 900 recommendations were submitted to the ICT Division.[21] A new draft was placed before the Cabinet six days after the deadline of 22 August for submission of feedback with minimal changes that retained the repressive sections of the DSA like the first draft of the CSA. Amnesty International and other rights groups, such as Transparency International, urged the Bangladeshi authorities yet again to remove the draconian provisions from the draft CSA before taking it any further and align it with international human rights law.[22] Amnesty International's legislative analysis found that the government made changes to 16 sections in the final version of the CSA, compared to the draft version which was published for public feedback.[23] Only two of these changes were substantive, while the remaining changes were minor terminological alterations.[24] Amnesty International believes, as do other civil society organisations and human rights defenders working in or on Bangladesh, that the call for feedback on the CSA draft was a mere tick box exercise since substantial recommendations made by civil society were completely ignored. Despite receiving such extensive feedback, the Parliament nevertheless enacted a law that is largely a replication of the DSA that preceded it and retains repressive features which have been used to threaten and restrict the rights to freedom of expression, privacy and liberty in Bangladesh. Its various overly broad provisions fail to meet the requirements of legality, necessity, and proportionality, and are therefore incompatible with international human rights law. The CSA continues to give legal cover to the authorities to police permissible expression online and can be used to intimidate, harass and arbitrarily arrest journalists and human rights defenders, stifle peaceful dissent and silence critical opinions.

[16] OHCHR, Technical Note to the Government of Bangladesh on review of the Digital Security Act (June 2022), paras 6, 8, 10, 12, 14, 16, 18, 20 and 22. https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf
[17] Amnesty International, *Muzzling Dissent Online* (previously cited).
[18] Amnesty International South Asia Regional Office, 7 August 2023, X (formerly Twitter), https://twitter.com/amnestysasia/status/1688494134934331392; Prothom Alo, "Govt must ensure Cyber Security Act doesn't rehash repressive features of DSA: Amnesty", 07 August 2023, https://en.prothomalo.com/bangladesh/lc37x1zp93
[19] The Daily Star, "Cyber Security Act: Stakeholders have to give opinions by August 22" 11 August 2023, https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-stakeholders-have-give-opinions-august-22-3391231
[20] Amnesty International, "Bangladesh: Open letter to the government: Feedback on proposed 'Cyber Security Act', 22 August 2023, https://www.amnesty.org/en/documents/asa13/7125/2023/en/
[21] The Daily Star, "Cyber Security Act: Most suggestions go unheeded", 29 August 2023, https://www.thedailystar.net/news/bangladesh/news/cyber-security-act-most-suggestions-go-unheeded-3405471
[22] Amnesty International, "Bangladesh: Government must remove draconian provisions from the Draft Cyber Security Act", 31 August 2023, https://www.amnesty.org/en/latest/news/2023/08/bangladesh-government-must-remove-draconian-provisions-from-the-draft-cyber-security-act ;Transparency International Bangladesh, Digital Security Act 2018 and the draft Cyber Security Act 2023 : A Comparative Analysis, https://www.ti-bangladesh.org/upload/files/position-paper/2023/Position-paper-on-Digital-Security-Act-2018-and-Draft-Cyber-Security-Act-2023.pdf
[23] A list of these changes is set out in the Annex 2 to this briefing.
[24] The two substantive changes are: Introduction of an offence for filing false cases (Section 34 of the CSA) and removal of the offence of breaching secrecy of the government (which was introduced under Section 32 of the DSA and retained in Section 32 of the draft CSA).

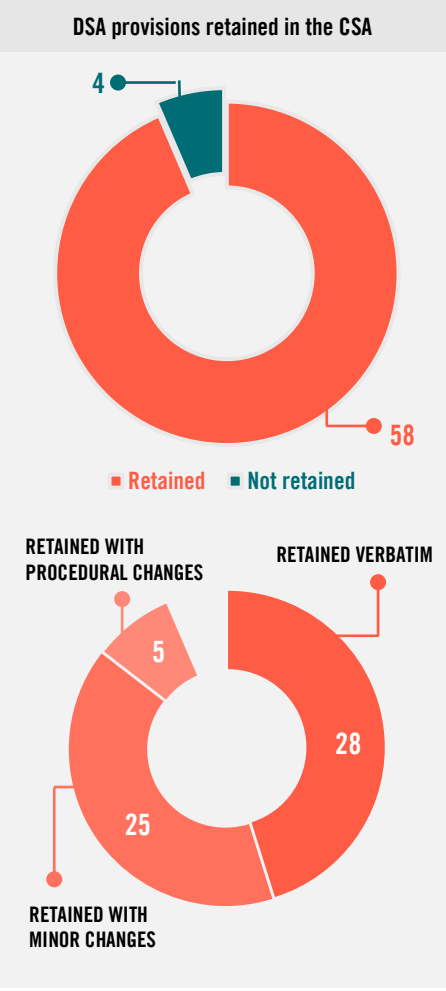
3. METHODOLOGY

This briefing presents Amnesty International's analysis of the newly enacted CSA in Bangladesh, the pattern of cases filed under it so far, and the enduring crackdown on the right to freedom of expression in Bangladesh through three main sources of data. First, it draws on legislative analysis which primarily entailed reviews of the newly enacted Cyber Security Act 2023, the first draft of the Cyber Security Act 2023, the Digital Security Act 2018 and the Information, Communication and Technology Act 2006 (amended 2013). Annex 1 provides a line-by-line comparative analysis of the CSA and the DSA, and Annex 2 lists the changes made in the final version of the CSA compared to the draft version published for public feedback. Second, it analyses cases known to be filed under the CSA, identified through open-source investigation, primarily from media reports. Third, it draws on 20 interviews conducted in March, April, August, October and November 2023 and February, March, April and May 2024, with a range of stakeholders, including former detainees, their relatives, their lawyers as well as journalists and human rights defenders in Bangladesh. While the vast majority (i.e. 16) of these interviews were conducted remotely, four were conducted in person in November 2023 and February 2024. The stakeholders whose testimonies have been used in this briefing have been anonymised to conceal their identity and ensure their security.

The text of this briefing was finalised on 10 July 2024. The findings reflect the state of affairs in Bangladesh as applicable on that date. The publication of this briefing was postponed from July 2024 to August 2024 due to the political crisis that unfolded in July 2024, which led to the resignation of Prime Minister Sheikh Hasina and her government on 5 August 2024. The findings and recommendations of this briefing reflect the urgency for Bangladesh to end the longstanding crackdown on dissent.

4. OVERVIEW OF CHANGES IN THE CSA

Amnesty International's legislative analysis has found that the CSA retains 58 of the 62 provisions of the DSA: 28 provisions are retained verbatim, while 25 provisions are retained with minor changes (such as those related to sentencing or terminological alterations).[25] The remaining five provisions of the DSA are retained in the CSA with some procedural changes.[26] The CSA adds only one new provision which is an offence for filing false cases.[27] Therefore, 58 of the 59 provisions in the CSA were inherited from the DSA, either verbatim or with minor changes or procedural alterations. Both the CSA and DSA have nine identical chapter headings. This section provides a chapter-wise summary of the key changes made by the CSA, when compared to the DSA. Since the provisions in the CSA remain entirely unchanged for Chapter 5 (Critical Information Infrastructure) and Chapter 8 (Regional and International cooperation), these two chapters are excluded from the overview below.



4.1 PRELIMINARY PROVISIONS

Chapter 1 contains preliminary provisions, such as the list of definitions. Most changes in this chapter were terminological or rudimentary. The only noteworthy change is the replacement of the definition of 'digital security' (i.e. the security of any digital device or digital system) in the DSA with a slightly wider definition of 'cyber security' which is 'the security of any digital device, computer, or computer system'.[28] By expanding the definition of cyber security to security of computers and computer systems, the CSA has wider implications and potential for encroachments on data

[25] For a line-by-line comparison of the DSA with the CSA, see the Annex 1 to this briefing.
[26] Sections 12, 40, 50, 53 and 61 of the DSA have been retained with some procedural changes in the following five sections of the CSA respectively: Section 12 (which slightly changes the membership composition of the National Cyber Security Council), Section 40 (which increases the time limit for investigation for cases filed under the CSA), Section 50 (which makes certain procedural provisions of the ICT Act applicable to cases filed under the CSA), Section 53 (which decreases the number of non-bailable and cognisable offences) and Section 61 (which introduces a broader savings clause). For a detailed analysis of these changes, see the Annex 1 to this briefing.
[27] CSA, Section 34.
[28] CSA, Section 2(v); DSA, Section 2(k).

privacy. This is because while 'digital system' was not defined in the DSA, 'computer system' is defined in the CSA as a 'process interconnected with one or more computers or digital devices capable of collecting, sending, and storing information singly or being connected with each other'.[29]

4.2 NATIONAL CYBER SECURITY AGENCY

Chapter 2 pertains to the establishment of the National Cyber Security Agency, a body with the wide mandate of 'carrying out the purposes of the Act'.[30] Earlier, the DSA had established the Digital Security Agency which the CSA now replaces with the Cyber Security Agency ('Agency').[31] A new provision in the CSA stipulates that the Agency will now be 'administratively attached' to the Information and Communication Technology (ICT) Division, a ministerial division under the Ministry of Posts, Telecommunications and Information. Since 2014, the prime minister's son has served as an 'honorary adviser' to the ICT Division, and in January 2024 was re-appointed as the ICT Adviser to the prime minister for the third consecutive time.[32]

4.3 PREVENTIVE MEASURES

Chapter 3 sets out the preventive powers of the Agency, the most significant of which is the power to remove or block data under Section 8. The Director General of the Agency can ask the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block data or information that 'threatens cyber security'. The CSA makes only one noteworthy amendment to Chapter 3, which is a minor change to the wording of Section 8, by introducing the need for the Director General to analyse data and have reasonable belief of harm before requesting the BTRC to remove any data or information.[33]

4.4 NATIONAL CYBER SECURITY COUNCIL

Chapter 4 pertains to the establishment and powers of the National Cyber Security Council, which provides 'necessary direction and advice to the Agency'.[34] Earlier the DSA had established the National Digital Security Council which the CSA now replaces with the National Cyber Security Council. The Council continues to be chaired by the prime minister and continues to have the power to give directions to the Agency and formulate inter-institutional policies on cyber security. The CSA makes only one significant amendment to this chapter by inserting a minor change to the membership composition of the Council, which continues to be made up entirely of representatives from the executive branch of the state. The CSA adds the heads of three other executive agencies to the membership of the Council, namely the Director General of the National Security Intelligence, the Director General of the National Telecommunication Monitoring Centre, and the Director General of the Agency.[35] As such, the CSA further entrenches executive influence and control over the Council. This level of executive control over the Council, without any judicial oversight, has serious implications for the rights to freedom of expression and privacy. The CSA also adds a new provision requiring the Director General of the Agency to provide secretarial assistance to the Council.[36] As noted above, the CSA makes no changes to Chapters 5 and 6.

[29] CSA, Section 2(e).
[30] CSA, Section 5.
[31] Chapter 2 of the CSA read with Section 59(4) of the CSA.
[32] The Business Standard, "Joy reappointed as PM's ICT adviser", 21 January 2024, https://www.tbsnews.net/bangladesh/sajeeb-wazed-joy-reappointed-pms-ict-adviser-778858
[33] CSA, Section 8(2).
[34] CSA, Section 13.
[35] CSA, Section 12(1).
[36] CSA, Section 12(2).

4.5 OFFENCES AND PUNISHMENT

Chapter 6 sets out all the offences under the Act. The CSA retains all the offences in the DSA, except for two. These are: 'breaching secrecy of the Government' and 'holding, transferring data-information illegally'.[37] The CSA also introduces one new offence, which is filing or causing someone to file a false case or complaint 'knowing that there is no just or legal ground'.[38] This offence is punishable by the penalty prescribed for the offence alleged in the false case or complaint. If the false case alleges offences covered by more than one section, then the alleged offence with the highest penalty will apply.

The CSA retains the 18 remaining substantive offences in the DSA verbatim (including the five authoritarian speech offences), and only makes sentencing-related changes to these offences, as shown in Table 1.[39] First, it removes the higher penalty applicable for repeat offenders for all 18 of these offences. Second, it reduces the maximum prison sentence for eight offences, while keeping it unchanged for eight other offences. Third, the CSA removes the custodial sentence for the two remaining offences. These are: defamation and unlawful e-transactions.[40] Fourth, the CSA decreases the maximum amount of fine leviable by 500,000 BDT (4,256 USD) for one offence i.e. hurting religious sentiments,[41] while it remains the same for 14 offences. For the three remaining offences, the CSA increases the fine by 2 million BDT (17,024 USD), two of these are the offences which no longer have a custodial sentence (i.e. defamation and unlawful e-transaction).

Table 1: Sentencing-related changes to substantive offences under the CSA in comparison to the DSA

Section	Offence	Change in Prison Term	Change in Fine Amount
17(2)(a)	Illegal access to critical information infrastructure	**-4 years**	Same
17(2)(b)	Illegal access to critical information infrastructure causing or attempting to cause harm, damage, or disruption	**-8 years**	Same
18(a)	Illegal access to computer, digital device or computer system	Same	Same
18(b)	Illegal access to computer, digital device, computer system with intent to commit offence	Same	Same
19	Damage of computer or computer system	Same	Same
20	Modification of computer source code	Same	Same
21	Campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag	**-3 years**	Same
22	Digital or electronic forgery	**-3 years**	Same
23	Digital or electronic fraud	Same	Same
24	Identity fraud or personation	Same	Same
25	Publishing offensive, false or threatening data- information	**-1 year**	Same
26	Unauthorised collection, use etc. of identity information.	**-3 years**	Same
27	Cyber terrorism	Same	Same

[37] DSA, Section 32 and 33. The first draft of the CSA had retained the former offence, but it was ultimately removed in the final version that was enacted.
[38] CSA, Section 34.
[39] The remaining provisions in Chapter 6 of the CSA are descriptive provisions which do not constitute substantive offences in and of themselves. These are: Sections 33 (abetment), 35 (offence committed by a company), 36 (power to issue order for compensation) and 37 (service provider not to be responsible).
[40] DSA, Section 29 and 30.
[41] DSA, Section 28.

28	Publishing information that hurts the religious values or sentiment	**-3 years**	-500,000 BDT
29	Defamation	**Removed**	**+2 million BDT**
30	E-transaction without legal authority	**Removed**	**+2 million BDT**
31	Deteriorating law and order to disrupt communal harmony, etc.	**-2 years**	**+2 million BDT**
32 (CSA) 34 (DSA)	Hacking	Same	Same

4.6 INVESTIGATION AND TRIAL OF OFFENCES

Chapter 7 pertains to the investigation and prosecution of offences under the Act. The CSA makes two positive changes to this chapter. First, eight offences, which were cognisable and non-bailable under the DSA, are now non-cognisable and bailable under the CSA. Therefore, the police can no longer arrest individuals accused of these offences without a warrant, while courts must grant them bail as a matter of right. Second, a provision in the DSA which allowed the time for investigation to be extended 'up to a reasonable period' after the investigating officer failed to complete it within the time limit, has not been retained by the CSA.[42]

Aside from these positive amendments, the CSA also makes some other procedural changes in this chapter. First, the maximum time-limit for investigation has been increased from 60 days under the DSA to 90 days under the CSA.[43] Second, the CSA also does not retain Section 50(3) of the DSA which required the person presenting the case in the Cyber Tribunal on behalf of the complainant to be regarded as the Public Prosecutor. Third, Section 49(2) of the CSA makes the procedural provisions related to investigation, trial and appeal etc. prescribed under Part-II and Part-III of Chapter VIII of the ICT Act applicable to cases under the CSA.[44] In this regard, Section 49(2) refers to six procedural matters that shall be governed by the provisions of the ICT Act, which roughly correspond to ten specific sections of the ICT Act, though these sections are not expressly mentioned in Section 49(2) of the CSA. These are: (a) Trial procedure of Tribunals and Appellate Tribunals (Sections 74 and 75, ICT Act), (b) Time limit to deliver judgment: (Sections 72 and 73, ICT Act), (c) Penalties or forfeiture no bar against other punishments (Section 78, ICT Act); (d) Power of detention or arrest in public place, etc. (Section 80, ICT Act); (e) Procedure of search (Section 81, ICT Act); and (f) Power of Appellate Tribunal and procedure for hearing and disposal of appeals (Sections 82-84, ICT Act). However, since Section 49(2) of the CSA does not expressly limit the applicability of the ICT Act to these ten sections, there is a risk that other sections of Part II and Part III of Chapter VIII of the ICT Act may also be applied to cases filed under the CSA. Two such sections are of particular concern.

Section 71 of the ICT Act limits the power of the Cyber Tribunal judge to grant bail by prescribing three preconditions. First, the Cyber Tribunal judge must ensure that the state party is afforded an opportunity for a hearing on such bail order. Second, the judge must be satisfied that there are reasonable grounds for believing that the accused may not be convicted on trial. Third, the judge must be satisfied that the offense is not serious in the relative sense and the punishment shall not be severe even if the offense is proved. Additionally, the judge must record in writing the reasons for such satisfaction. Therefore, this provision may continue to limit the prospect of bail in cases under the CSA despite the law increasing the number of bailable offences compared to the DSA.

Section 80 of the ICT Act grants sweeping powers of detention and arrest to police officers if they have 'reason to believe that any act contrary to this Act has been or is being committed in any place' or if any crime punishable under the law has been committed. The police may enter and search the place after recording reasons for their belief and 'may seize anything concerned and arrest any person or criminal concerned'. Although the CSA did not retain Section 41 of the DSA which granted wide powers of

[42] DSA, Section 40(2).
[43] DSA, Section 40 cf CSA, Section 39.
[44] CSA, Section 49(2).

seizure to the investigating officer, even broader powers of arrest and seizure are now granted under Section 80 of the ICT Act.

4.7 MISCELLANEOUS PROVISIONS

Chapter 9 is the final portion of the Act which sets out miscellaneous provisions. The CSA does not retain Section 57 of the DSA, which had exempted employees of the Agency and any other person from prosecution, civil action, or any other legal proceedings for any damage caused to any individual due to the exercise of any actions under the DSA, provided it was done in good faith.

Section 59(2) of the CSA allows pending cases under the DSA to be conducted and disposed of as if the DSA had not been repealed. Pending DSA cases include not only those which were under trial before the Cyber Tribunal at the time of the repeal, but also those cases in the pre-trial stage i.e., where a report or complaint has been made or a charge sheet has been submitted or where the case is under investigation.[45] This 'savings' clause allows the state to continue framing charges and making arrests under the DSA, as Section 6 of this briefing will show.

[45] CSA, Section 59(2) and 59(3).

5. THE ONGOING THREATS TO FREEDOM OF EXPRESSION UNDER THE CSA

As the legislative analysis in the preceding section has shown, the CSA can hardly be characterised as a new law. It is essentially the same piece of legislation as the DSA, with some minor amendments. The CSA retains most of the repressive provisions of the DSA which have persistently been used to threaten and restrict the right to freedom of expression in Bangladesh. As one journalist explained to Amnesty International:

"The massive campaign against DSA at the national and international levels forced the government to distance itself from the DSA by putting on a performance of introducing a new law in its place. You can take the D out of DSA and add C to make it CSA. But it is the same. The fear is there. If you cross the line, they will use the CSA just like they used the DSA to strangle your throat."

The CSA, just like the DSA, and the ICT Act that preceded it, can and has been used to clampdown on peaceful dissent and silence critical opinions.[46] Both Article 19 of the ICCPR and Article 39 of the Constitution of Bangladesh recognise that the right to freedom of expression is subject to permissible restrictions. However, the restrictions posed by CSA, like the restrictions imposed by the DSA before it, are impermissible, as they fail to meet the requirements of legality, necessity, and proportionality, and therefore incompatible with international human rights law.[47] The only grounds on which the right to freedom of expression may be restricted are set out in Article 19(3) of the ICCPR: "(a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals", and in order to be lawful, any such restrictions must be provided by law and meet the requirements of necessity and proportionality. In August 2023, after the draft CSA was published for public feedback, the UN Special Rapporteur on Freedom of Expression (SR FOE) wrote to the Government of Bangladesh, urging it to incorporate the OHCHR recommendations into the draft CSA, and providing further guidance on how to do so to bring the draft law in line with international

[46] Amnesty International, *No Space for Dissent* (previously cited); Amnesty International, *Bangladesh: Muzzling Dissent Online* (previously cited); Amnesty International, *Caught between fear and repression* (previously cited). For a discussion on the use of the CSA, see Section 7 of this briefing.
[47] For a discussion of this incompatibility with International Human Rights Standards, see Sections 5.1, 5.2, 5.3 and 5.4 of this briefing below.

standards.[48] Regrettably, as the legislative analysis in the previous section makes clear, the Government of Bangladesh has only implemented one of the eight recommendations of the OHCHR in the CSA (Table 2). This is the removal of Section 32 which referred to the crime of 'breaching secrecy of the Government' for committing or abetting offences under the colonial Official Secrets Act 1923,[49] 'by means of computer, digital device, computer network, digital network or any other digital means'.[50] It has partially implemented three recommendations, while the remaining five recommendations have been completely ignored in the CSA (Table 2).[51]

The next subsection considers each of these outstanding areas of concern in the CSA and how they continue to pose a threat to the right to freedom of expression and violate international human rights standards.

Implementation of OHCHR recommendations

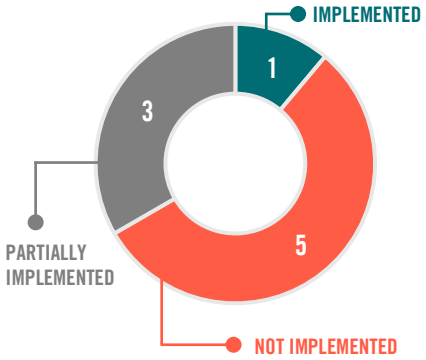


Table 2: Implementation status of OHCHR recommendations on the reform of DSA in CSA

OHCHR recommendation	Implementation status in CSA
Repeal Section 21	Not implemented
Repeal Section 28 and provide redress to those previously sanctioned under it	Not implemented
Decriminalise defamation under Section 25 and 29	Partially implemented, with removal of custodial sentence for offences under section 29.
Amend Section 31 so it penalises speech within the narrow scope of incitement to hatred	Not implemented, the scope and framing of Section 31 remains exactly the same except for sentencing related changes.
Amend section 27 to bring it in line with the narrow definition of terrorism as defined by the Special Rapporteur on counter-terrorism and human rights	Not implemented, the scope and framing of section 27 remains exactly the same except for removal of higher penalty applicable to repeat offenders.
Amend Section 32 to bring it in line with Article 19 of the ICCPR	Implemented. The CSA does not retain Section 32.
Amend Section 8 to more narrowly define the bases upon which data-information may be blocked or removed by the Digital Security Agency	Partially implemented. CSA makes a minor change to the wording of Subsection 8(2) which introduces the need for the Director General of the Cyber Security Agency to analyse data and have reasonable belief of harm before requesting it to be removed.
Amend Section 43 to ensure that the powers of investigating officers are clear and well defined	Not implemented. The scope and framing of Section 43(1) remain exactly the same, except addition of references to computer system in section 43(1), which broadens its scope.
Amend Section 53 and the Act so that release pending trial is the general rule and bail conditions are specified etc.	Partially implemented. Seven out of the 11 offences which used to be non-bailable and cognisable under the DSA are now bailable and non-cognisable offences under the CSA. However, the remaining four offences remain cognizable and non-bailable under the CSA while bail conditions are specified in Section 81 of the ICT Act which is now applicable to CSA cases.

[48] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL BGD 7/2023, 28 August 2023, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=28358
[49] Official Secrets Act 1923, http://bdlaws.minlaw.gov.bd/act-details-132.html
[50] DSA, Section 32.
[51] These three recommendations are the ones to decriminalise defamation under Sections 25 and 29, amend Section 8 and amend Section 53 of the DSA.

5.1 THE FIVE AUTHORITARIAN SPEECH OFFENCES

As noted in the previous section, the CSA retains verbatim all five authoritarian speech offences which had been weaponised by the Bangladeshi government under the DSA to stifle peaceful dissent and set draconian limits on the parameters of acceptable speech. The CSA leaves the substance of these offences completely unchanged, while only reducing the applicable penalties and removing provisions mandating higher punishment for repeat offenders. In 2021, Amnesty International had documented an alarming pattern whereby three of these authoritarian speech offences under the DSA i.e. Sections 25 (publish false or offensive information etc.), 29 (defamation) and 31 (deteriorate law and order or disrupt communal harmony), had been especially weaponised to target and harass dissenting voices, including those of journalists, human rights defenders (HRDs) and activists.[52] Amnesty International found that eighty percent of cases relating to DSA recorded by the Cyber Tribunal in Dhaka between 1 January and 6 May 2021 were filed under Sections 25 and 29 of the DSA to criminalise 'false, offensive, derogatory and defamatory information', in contravention of the ICCPR.[53] As noted earlier, in 2018, Amnesty International had raised concerns about the sweeping nature of these offences ever since the enactment of the DSA, and recommended that these be repealed or amended in line with international human rights law.[54] In retaining the five speech offences, the potential to weaponise these provisions to silence peaceful dissent, as done under the DSA, remains unchanged. This subsection analyses each of these five offences, the tokenistic changes made to them by the CSA and their enduring non-compliance with international human rights standards. Although two of these speech offences i.e. hurting religious sentiments[55] and defamation, [56] also existed in the colonial Penal Code 1860, the penalties were lower and cases were much rarer.[57]

5.1.1 FALSE OR OFFENSIVE INFORMATION

SECTION 25 OF THE CSA

'Transmission, publication, etc. of offensive, false or threatening data- information

(1) If any person, through any website or any other digital medium, (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 (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, then such act of the person shall be an offence.

(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 3 (three) lac, or with both.'

Section 25 of the Act is not just alarming because it contains vague and undefined terms that may be prone to abuse, but also because it affords special protection to the state and thus may be used to prohibit or punish legitimate political expression. The Act includes a crime of disseminating data, which it defines as 'invasive', 'intimidating', 'being well-known lie', with the intention of 'annoying, insulting or humiliating'. The way Section 25 is drafted has allowed the state to criminalise legitimate expression of either opinion or facts relating to all manner of political, scientific, historic, religious or moral issues.[58] The vague and overbroad terms used in Section 25 (such as 'affect the image or reputation of the state' or 'spread confusion') remain undefined in the list of definitions in section 2 or elsewhere in the CSA. Therefore, the terms could be misused or interpreted in a manner contrary to the requirements of international human rights law, as has been the case under the DSA. For instance, highlighting or reporting violations of international human rights standards by state agencies can easily be construed as affecting 'the image or reputation of the state' and therefore criminalised under the CSA. Similarly,

[52] Amnesty International, *No Space for Dissent* (previously cited), pp. 16-17.
[53] Amnesty International, *No Space for Dissent* (previously cited), pp. 17.
[54] Amnesty International, *Bangladesh: Muzzling dissent online* (previously cited).
[55] Penal Code 1860, Section 295A (Deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs) and Section 298 (Uttering words, etc., with deliberate intent to wound religious feelings).
[56] Penal Code 1860, Section 500 (Punishment for defamation).
[57] Interview by video call with a Senior Advocate of the Supreme Court of Bangladesh (name withheld for security reasons), 3 May 2024.
[58] Amnesty International, *No Space for Dissent* (previously cited).

'annoy', 'insult', 'humiliate' and 'spread confusion', are other vague and overly broad terms used in Section 25 which also remain undefined. Due to the broadly worded nature of Section 25, it can and has acted as a catch-all provision to criminalise a wide range of conduct which consists of the legitimate exercise of the right to expression and opinion. For instance, in February 2021, rights activist Ruhul Amin was arrested for a Facebook post criticizing the Bangladeshi government and Prime Minister Sheikh Hasina for the death of Mushtaq Ahmed. Using reference of the post, the Detective Branch accused Ruhul Amin of "tarnishing the image of the state as well as the government, using propaganda to create confusion, hate, unrest and animosity among public and attempting to deteriorate law and order" under sections 25(2) and 31(2) of the DSA.[59] Since the CSA leaves the overbroad language of Section 25 unchanged from the DSA, critics and dissidents remain susceptible to similar retaliation.

5.1.2 DETERIORATING LAW AND ORDER

SECTION 31 OF THE CSA

'Offence and punishment for deteriorating law and order, etc.

(1) If any person intentionally publishes or transmits anything in website or digital layout that creates enmity, hatred or hostility among different classes or communities of the society, or destroys communal harmony, or creates unrest or disorder, or deteriorates or advances to deteriorate the law-and-order situation, then such act of the person shall be an offence.

(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both.'

Although termed 'deteriorating law and order', Section 31 continues to contain overbroad provisions criminalizing content that 'creates hostility, hatred or prejudice among different classes or communities' or 'destroys communal harmony or creates unrest or disorder or deteriorates law and order'. It is precisely the lack of clear definitions for these broad terms that allowed arbitrary application of this provision under the DSA.[60] As one lawyer explained, Section 31 is so broadly worded that it has become the 'add on' provision whereby it can be coupled with any of the other four speech offences. OHCHR had recommended that section 31 be amended to comply with article 20 of the ICCPR, so that speech is only criminalised within the narrow scope of incitement to hatred.[61] The CSA reduces the maximum prison sentence for convictions under Section 31 from seven years to five years but introduces a five-fold increase in the maximum fine leviable from 500,000 BDT (4,256 USD) to 2.5 million BDT (21,280 USD).

5.1.3 HURTING RELIGIOUS SENTIMENTS

SECTION 28 OF THE CSA

'Publication, broadcast, etc. of information in website or in any 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 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.

(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 5 (five) lac, or with both.'

[59] Amnesty International, *No Space for Dissent* (previously cited).
[60] Amnesty International, *No Space for Dissent* (previously cited); Amnesty International, "Bangladesh: Teenage girl detained for Facebook post: Dipti Rani Das", 12 November 2018, https://www.amnesty.org/en/documents/asa13/9364/2018/en/; Amnesty International, "Bangladesh: Man faces 7 years in prison for Facebook post: Emdadul Haque Milon", 1 March 2020, https://www.amnesty.org/en/documents/asa13/1945/2020/en/
[61] OHCHR, Technical Note to the Government of Bangladesh on review of the Digital Security Act (previously cited).

CSA similarly retains Section 28 of the DSA verbatim which criminalises any speech that 'hurts the religious values or sentiment'. The only qualifier for this broad offence remains that the act must be carried out with the knowledge of or intention to hurt or provoke religious values or sentiments. Although Section 295A of the colonial Penal Code 1860 also has a comparable offence which criminalises 'deliberate and malicious acts intended to outrage religious feelings', courts could only take cognizance of this offence if the complaint was made by order of, or under authority from, the government, or some officer empowered by the government.[62] This procedural restriction significantly limited the number of cases that could be filed under Section 295A of the Penal Code, when compared to cases filed for hurting religious sentiments under Section 28 of the DSA and CSA.[63]

The right to freedom of expression extends even to statements that are deeply offensive.[64] Moreover, 'the right to freedom of religion or belief, as enshrined in relevant international human rights instruments, does not include the right to have a religion or a belief that is free from criticism or ridicule'[65] and 'subjective feelings of offensiveness... should never guide legislative action, court decisions or other State activities.'[66] The ICCPR requires the prohibition – but not necessarily the criminalization – of only the narrow category of expression that amounts to 'advocacy of... hatred that constitutes incitement to discrimination, hostility or violence.'[67] However, Section 28 does not fit within this narrow exception on incitement, which Section 31 can and should be amended to cover. It is for this reason that the OHCHR recommended that Section 28 be repealed in its entirety.[68] The punishment for offences under Section 28 has been reduced from up to five years' imprisonment and/or a 1 million BDT (8,512 USD), to up to two years' imprisonment and/or 500,000 BDT (4,256 USD) fine. However, it continues to criminalise protected speech.

5.1.4 PROPAGANDA AGAINST THE SPIRIT OF LIBERATION WAR

> **SECTION 21 OF THE CSA**
>
> **'Punishment for carrying out any hateful, confusing and defamatory campaign about liberation war, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag.**
>
> (1) If any person, by means of digital or electronic medium, carries out or instigates to carry out any propaganda or campaign against the liberation war of Bangladesh, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag, then such act of the person shall be an offence.
>
> (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 1 (one) crore, or with both.'

Section 21, which criminalises making any kind of propaganda or campaign against the spirit of liberation war etc., is the only offence where CSA makes some, albeit minor, changes to the formulation of the offence. Firstly, the description of the offence now includes new broad terminologies such as 'hateful', 'confusing' and 'defamatory' and explicit reference to Bangabandhu Sheikh Mujibur Rahman as the father of the nation. Secondly, reference to 'electronic medium' has been included in addition to 'digital' medium as places where the offence may take place. The definition of the term 'the spirit of liberation war' in Chapter 1 is largely similar under the CSA as the DSA: 'nationalism, socialism, democracy, and secularism which are the ideals which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle'.

According to Article 19(1) of the ICCPR, all forms of expression are protected, be they political, religious, historic, scientific, or moral. The Human Rights Committee has clearly stated that laws that

[62] Code of Criminal Procedure 1898, Section 196.
[63] Interview by video call with a Senior Advocate of the Supreme Court of Bangladesh (name withheld for security reasons), 3 May 2024.
[64] UN Human Rights Committee, General Comment 34: Article 19: Freedoms of opinion and expression, 12 September 2011, UN Doc. CCPR/C/GC/34, para. 11.
[65] The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, A/HRC/22/17/Add.4, para. 19.
[66] Report of the Special Rapporteur on freedom of religion or belief, Un Doc. A/HRC/31/18, para. 61.
[67] ICCPR, Article 20(2).
[68] OHCHR, *Technical Note to the Government of Bangladesh on review of the Digital Security Act* (previously cited).

penalise the expression of opinions about historical facts are incompatible with Article 19 of the ICCPR.[69] It has stated that 'The Covenant does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events'.[70] The manner in which section 21 is drafted is clearly contrary to the obligations of the government of Bangladesh under the ICCPR, in that it generally prohibits and criminalises what it terms 'propaganda or campaign' on historical facts or political facts. The concept of the right to freedom of expression protects both the right to hold such opinion and to express an opinion on any of the grounds of political, religious, historic, scientific or moral opinion or belief. The only restriction can be in terms of Article 20 where prohibitions are permitted on grounds of incitement to hatred, and where such prohibition meets the three-part test set out in Article 19(3), as mentioned above. Section 21 of the Act does not meet the exceptions set out in the ICCPR for such restrictions. Although the CSA reduces the maximum prison sentence for convictions under Section 21 from ten years to five years, it keeps the maximum fine leviable at an astonishingly high level of 10 million BDT (80,512 USD).

5.1.5 DEFAMATION

> **SECTION 29 OF THE CSA**
> 'Publication, transmission, etc. of defamatory information.
>
> (1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format, then the act of such person shall be an offence, and for this, he shall be punished with fine not exceeding Taka 25 (twenty-five) lac.'

Defamation has been criminalised since the colonial era under Sections 499 and 500 of the Penal Code 1860, punishable by up to two years imprisonment and/or fine. The DSA had introduced defamation as a separate offence under Section 29 with the same meaning as defined under the Penal Code but with higher punishment i.e. up to three years imprisonment and/or up to 500,000 BDT (4,256 USD) fine. Since then, the number of defamation cases filed under Section 29 in comparison to cases under the Penal Code.[71] As one news editor with 20 years of experience in print media explained, 'in the early days, we had to be mindful of the risk of a defamation case being filed under the Penal Code. However, as long as our documents were in order, we knew we could go ahead with the story. Then the ICT Act came, and since then, slowly but surely we were bulldozed into a culture of censorship where the limits of permissible reporting is becoming narrower and narrower.'

Amnesty International has repeatedly called for the full decriminalization of defamation in Bangladesh.[72] The UN Human Rights Committee has similarly advised States to avoid 'penalizing or rendering unlawful untrue statements that have been published in error but without malice'.[73] The OHCHR has urged the government of Bangladesh to replace 'criminal defamation laws with civil laws that are more narrowly defined and include defences, such as the defence of truth or a defence for public interest in the subject matter of the criticism'.[74]

Although the CSA removes the custodial sentence for defamation under Section 29, it applies a five-fold increase to the maximum leviable fine from 500,000 BDT (4,256 USD) to 2.5 million BDT (21,280 USD) as it has also done for Section 31). When the draft CSA was published for public feedback, at a press conference the law minister specifically highlighted this change as a progressive one and stated 'Prime Minister Sheikh Hasina's government is working as a listening government. That is why this decision has been taken.'[75] However, defamation remains criminalised under CSA, with a much heftier maximum fine, and the scope of imprisonment remains under the Penal Code.

[69] UN Human Rights Committee, General Comment No. 34 (previously cited), para. 49.
[70] UN Human Rights Committee, General Comment No. 34 (previously cited), para. 49.
[71] Interview by video call with a Senior Advocate of the Supreme Court of Bangladesh (name withheld for security reasons), 3 May 2024.
[72] See for example: Amnesty International, Bangladesh: Open letter to the government (previously cited).
[73] UN Human Rights Committee, General Comment No. 34 (previously cited), para 47.
[74] OHCHR, *Technical Note to the Government of Bangladesh on review of the Digital Security Act* (previously cited).
[75] Dhaka Tribune, "Minister: No jail terms in defamation cases under new law", 07 August 2023, https://www.dhakatribune.com/bangladesh/321828/minister-no-jail-terms-in-defamation-cases-under

5.2 OVERBROAD POWERS OF ARREST, SEARCH, AND SEIZURE

Amnesty International welcomes the reduction in the number of cognizable and non-bailable offences in CSA in comparison to the DSA. However, the offences covered by four sections of the DSA remain cognizable and non-bailable under Section 52 of the CSA. These are: Sections 17 (illegal access to any critical information infrastructure), 19 (Damage of computer, computer system), 27 (cyber terrorism) and 32 (hacking). This means that the police can continue arresting individuals without obtaining a court warrant for these four offences under the CSA, and the possibility of bail in such cases will also be severely restricted. This perpetuates the risk of arbitrary arrest and pre-trial detention for individuals accused under these sections, as the cases of Selim Khan and Shamim Ashraf discussed in Section 7 of this briefing will show.

More worryingly, Section 42 of the CSA is identical to Section 43 of the DSA and continues to authorise any police officer to search premises, to seize computers and similar hardware, and to search the body of a person and to arrest a person present in that place – without a warrant.[76] The police need only show that one of two overly permissive conditions existed to conduct such invasive search, seizure, or arrest. The police officers must believe that (a) a crime under the Act has occurred, is occurring or is likely to occur or (b) any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way.[77] They are simply required to record the reasons for such belief.[78] The OHCHR has cautioned that such 'unfettered discretion' under Section 43 of the DSA is contrary to the recommendations of the Human Rights Committee and powers of investigating officers must be clear and well defined to prevent misuse.[79] Therefore, despite the progressive conversion of previously cognizable offences under the DSA to non-cognizable offences under Section 53 of the CSA, the police may always resort to the broadly worded powers under Section 43 to make arrests without warrants where it pleases. Additionally, Section 40 of the CSA is verbatim to Section 41 of the DSA, and grants the investigating officer the power to confiscate computers, computer programs, systems, networks, digital devices and any program or information data that is stored on a retrieval system or in any other way. Given that this blanket power of confiscation is not subject to any conditions or judicial overview, there is a real danger of invasive investigations that may violate the right to privacy or other human rights.

Moreover, there are no clear safeguards on how the authorities should use and store the data in seized computers and similar hardware. According to existing international standards on combatting cyber-crime, such as the Convention on Cybercrime,[80] the investigative powers of law enforcement authorities (e.g. search and seizure of computer data) must be subject to clear safeguards.[81] These safeguards must ensure adequate protection of human rights and liberties guaranteed under other international treaties, such as the ICCPR, and include judicial or other independent supervision.[82] In its first substantial pronouncement by the UN on the right to privacy and surveillance, the UN warned against the capacity of governments to undertake surveillance, interception and data collection, which may violate or abuse human rights, particularly the right to privacy guaranteed under Article 17 of the ICCPR.[83] There must be clear regulation on how such data will be handled or destroyed at the conclusion of an investigation or trial.[84] The law should also clarify how the seized computer or hardware will be returned to its owner.

---

[76] Section 42 of the CSA states: '(1) If any police officer has reasons to believe that an offence under this Act has been or is being committed, or is likely to be committed in any place, or any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way, then he may, for reasons of such belief to be recorded in writing, proceed with the following measures, namely: - (a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure; (b) to seize the computer, computer system, computer network, data-information or other materials used in committing the offence or any document supportive to prove the offence; (c) to search the body of any person present in the place; (d) to arrest any person present in the place if the person is suspected to have committed or be committing an offence under this Act. (2) After concluding search under sub-section (1), the police officer shall submit a report on such search to the Tribunal.'

[77] CSA, Section 42(1).

[78] CSA, Section 42(1).

[79] OHCHR, *Technical Note to the Government of Bangladesh on review of the Digital Security Act* (previously cited).

[80] Budapest Convention on Cybercrime 2001, Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention. Although several non-member states of the Council of Europe has ratified the Budapest Convention, Bangladesh is not one of them. However, since the Budapest Convention is the first and only international convention on the combatting cyber-crime currently in force, this therefore makes it a useful point of reference. The UN is currently drafting a legally-binding international treaty to counter cybercrime. See: UN News, "Global Cybercrime Treaty: A delicate balance between security and human rights" 25 February 2024, https://news.un.org/en/interview/2024/02/1146772.

[81] Article 19 of the Budapest Convention on Cybercrime read with Article 15 of the Budapest Convention on Cybercrime.

[82] Budapest Convention on Cybercrime, Article 15.

[83] The right to privacy in the digital age, UN Resolution 68/167, UN General Assembly (2013). See also: Carly Nyst and Tomaso Falchetta, "The Right to Privacy in the Digital Age" Journal of Human Rights Practice (2017), https://academic.oup.com/jhrp/article-abstract/9/1/104/2965689

[84] UN Office of the High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, Un Doc. A/HRC/39/29, 3 August 2018, para. 37.

One senior law professor explained the inherent risks due to the lack of safeguards regulating the scope of investigative powers:

"The standard rule is when data from a device is seized by a state authority, the storage must be completed in the presence of a witness, the bearer of the data, who must be provided a right protected copy of the seized data which cannot be changed. This way, the seized data produced by the investigation or prosecution can be matched later with the right protected copy, so there is no scope of data manipulation. It has been over ten years since the ICT Act specifically empowered the state to seize data, but where are the safeguards on how such power should be fairly exercised? They have not yet been introduced and so the police have the liberty to do as they please."

One senior lawyer cautioned about the lack of digital forensic analysts in the country: "I have been told by multiple district court practitioners that there are only two digital forensic analysts who are not affiliated with the police and could potentially serve as defense witnesses. So even if an accused has a plausible defence, they would be unable to produce the expert witness needed to substantiate on that defence." The requirement to provide the right protected copy to experts for examination as evidence to be used in the trial is also mired by lack of independence. The police tend to get the seized data tested in a forensic lab which is under the Criminal Investigation Division, a specialised intelligence wing under the police.[85] This raises concerns about the impartiality and transparency of the forensic lab and the lack of judicial oversight on the overall process. The establishment of digital forensic labs under the CSA (like under the DSA), relies on the National Cyber Security Council, which not only has the power to control and supervise newly established labs under the Act, but also those labs established before the law was enacted.[86] As noted previously, the Council is chaired by the Prime Minister. As such, the law professor queried: "The government is the investigator, the data seizer, the forensic lab producer, and the prosecutor. Where is the transparency?"

5.3 OVERBROAD POWERS TO BLOCK AND REMOVE DATA

As noted in the fourth section of this briefing, Section 8 of the DSA had established the Digital Security Agency, which is now known as the Cyber Security Agency under the CSA ('the Agency'). The Agency is empowered with a wide mandate in terms of various offences under the Act. As noted above, this Agency is under the control and supervision of the National Digital Security Council, now named the Cyber Security Council ('the Council') under the CSA, which is chaired by the Prime Minister. Under Section 8(1) of the CSA, the Agency can request the removal or blocking of information and data if it believes that such information or data 'creates threat to digital security'. Not only is this provision vague, it also gives the power to the Agency to make blanket requests on the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove and block information and data on nothing more than their own assessment of a situation. In 2001, the BTRC was established through statute as 'an independent Commission for the purpose of development and efficient regulation of telecommunication system and telecommunication services in Bangladesh and matters ancillary thereto'.[87] As noted above, the CSA merely renames the Agency and the Council but keeps their mandate and powers identical.

Section 8(2) of the DSA (and now CSA) affords wide powers, this time to law enforcement forces, to request the BTRC to remove or block data, if it appears to them that such information hampers the country's or any part of the country's (a) solidarity (b) financial activities (c) security (d) defence (e) religious values or (f) public discipline or (g) incites racial prejudice and hatred. In such instances, law enforcement forces may make this request to the BTRC through the Director General of the Agency. The only change CSA makes to Section 8 is in subsection (2) by requiring the law enforcement agencies to have 'reason to believe' that any of these conditions are met 'subject to the analysis of data'. However, this remains a purely subjective assessment.

In rehashing these provisions of the DSA almost verbatim, the power to block or remove data remains repressive on several levels. The way Section 8 is drafted does not allow for a review of objective criteria in order to impose restrictions on freedom of expression; in fact, a decision by a law enforcement agency,

[85] Interview over a voice call with a senior law professor from Bangladesh (name withheld for security reasons), 7 May 2024.
[86] CSA, Section 10.
[87] Preamble to the Bangladesh Telecommunication Act 2001, https://ptd.portal.gov.bd/sites/default/files/files/ptd.portal.gov.bd/page/508a35d2_177c_4c29_adec_6c04c39e6464/Telecommunication_Act_2001.pdf

without any judicial oversight or opportunity to appeal the process, is sufficient to block websites or other digital means of sharing information and data. Although rhetorically termed a 'request' to remove or block data, Section 8(3) makes it clear that any such request from the Agency or law enforcement forces is binding on the BTRC since it 'shall' 'instantly remove' or 'block the data'. Allowing a government-controlled agency the power to essentially force a regulatory body to remove or block data nullifies the latter's independence granted by statute. As the law professor explained when speaking to Amnesty International: "Previously, the powers to remove and block data lay exclusively with the BTRC, an independent commission. The DSA tactfully allowed the government to usurp this power of the BTRC. How does it make sense for an independent commission to now become bound to comply with the command, or 'request' as it is called, of an external agency? And who constitutes this agency? No one knows. But we know who controls the agency, and that is the council. And who controls the council? None other than the prime minister."[88]

The problematic nature of the unchecked power to remove or block content is compounded by the vague and undefined aims for which the Act allows such removals or blocking. For a restriction on the right to freedom of expression to be consistent with international human rights law, it must – inter alia – 'be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly.'[89] The lack of definition of terms such as the country's 'solidarity', 'financial activities', 'defence' or 'religious values' leaves room for abuse. The vagueness of these terms, with no definitions provided, coupled with the mandatory blocking of such data on request by the Agency, creates a serious concern for guarantee of the right to freedom of expression.

Bangladeshi authorities have a long history of blocking news websites whenever they wish to suppress critique, not only from national outlets, but more importantly from international portals which have the scope to be bolder.[90] In November 2017, the BTRC ordered all international internet gateway operators to block the Indian news site The Wire, after it received a request from law enforcement agencies.[91] This order came a day after The Wire had published an article on the role of Bangladesh's military intelligence agency in the illegal pick-up and secret detention of a university academic. In December 2018, shortly after the enactment of the DSA and introduction of the Agency two months prior, the BTRC blocked 54 news sites for spreading 'anti-government propaganda and fake news' and ensuring 'national security' ahead of the general elections.[92] Then in February 2019, the government mandated for all internet service providers to install Deep Packet Inspection (DPI) equipment, which can be used to block or surveil internet traffic, by February 2019.[93] In the same month, Bangladeshi authorities blocked 20,000 websites describing it as a 'war against pornography', but the ban also included popular blogging sites and social media pages.[94] In March 2019, the Bangladesh government blocked Al Jazeera's English news website hours after it published an article detailing the alleged involvement of the country's defence chief in the enforced disappearance of three men.[95]

More recently, in January 2023, the government ordered the websites of 191 news portals to be shut for spreading 'anti-state propaganda'.[96] The transfer of the wide powers to block or remove data from the BTRC to the Agency in the DSA, and the retention of these provisions in the CSA, can be viewed as a concerted attempt by the government to maintain a stranglehold on news outlets. As one lawyer explained to Amnesty International in May 2024: "One of the main yet often unacknowledged purposes of the DSA was to create an agency, directly under the control of the government, with near total power to block and remove data from the cyberspace. We remember when the government blocked news sites such as The Wire, Netra News and Bdnews24 whenever they published a report highlighting human

[88] Interview over a voice call with a senior law professor from Bangladesh (name withheld for security reasons), 7 May 2024.
[89] UN Human Rights Committee, General Comment 34 (previously cited), para. 25.
[90] Interview over a voice call with a senior news editor from Bangladesh (name withheld for security reasons), 2 April 2023; Interview in person with a senior human rights defender from Bangladesh (name withheld for security reasons), 12 November 2023, Geneva; Interview over a voice call with a senior law professor from Bangladesh (name withheld for security reasons), 7 May 2024. See also: Human Rights Watch, "Bangladesh: Online Surveillance, Control", 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control
[91] David Bergman and Tasneem Khalil, "Bangladesh Government Blocks The Wire", The Wire, 25 November 2017, https://thewire.in/external-affairs/bangladesh-government-blocks-wire
[92] Reporters Without Borders (RSF), "RSF decries blocking of 54 Bangladeshi news sites before election", 12 December 2018, https://rsf.org/en/rsf-decries-blocking-54-bangladeshi-news-sites-election
[93] Human Rights Watch, "Bangladesh: Online Surveillance, Control", 8 January 2020, https://www.hrw.org/news/2020/01/08/bangladesh-online-surveillance-control.
[94] France 24, "Bangladesh shuts 20,000 websites in anti-porn 'war'", 19 February 2019, https://www.france24.com/en/20190219-bangladesh-shuts-20000-websites-anti-porn-war; Arab News, "Bangladesh shuts down popular blogging site in crackdown", 27 February 2019, https://www.arabnews.com/node/1458846/media.
[95] David Bergman and Tasneem Khalil, "Bangladesh blocks access to Al Jazeera news website", Al Jazeera, 22 March 2019, https://www.aljazeera.com/news/2019/3/22/bangladesh-blocks-access-to-al-jazeera-news-website
[96] The Daily Star, "191 news sites to be blocked over anti-state propaganda: info minister", 30 January 2023, https://www.thedailystar.net/news/bangladesh/governance/news/191-news-sites-be-blocked-over-anti-state-propaganda-info-minister-3234496

rights violations by the state or corruption by state officials. They have shown us time and time again that if any news portal crosses the limits of permissible speech set by the authorities, they can block their website instantaneously. Through this agency the government wields full power to decide what can and cannot be said in the cyber world, with utmost control but not the least bit of accountability or transparency." Blocking is a quasi-judicial power which should not reside with an executive agency. The power to block websites must be subject to judicial oversight. Even in emergency cases, the owners of the website need to be provided sufficient notice of the removal of data and they should have the right to challenge this in the judicial forum.

5.4 OVERBROAD DEFINITION OF CYBER-TERRORISM

"Cyber-terrorism" under the CSA (like under the DSA) remains a vague and imprecise offence which may be misused and abused.[97] The phrase 'intention to... creating fear among the public' in its definition is vague and unspecified and may be used against those who legitimately exercise their right to freedom of expression. The section also ascribes the crime to any person who either 'restrains legitimate access' or helps someone else illegally access any 'computer or computer network or internet network'. The way this section is drafted may allow application of this section to non-criminal acts. For example, it may apply to someone who allows another person to access his/her password, since the actus reus of intention to 'end state integrity, security and sovereignty' or even 'creating fear among the public' is vague and undefined. Therefore, the determination of what constitutes 'cyber-terrorism' remains extremely vague and subject to abuse, especially given the heavy punishments ascribed to this crime. Punishment for cyber-terrorism remains unchanged under the CSA with it being up to 14 years' imprisonment and/or a 1 million BDT (85,120 USD) fine.

[97] Section 27(1) of the CSA states: 'If any person (a) creates obstruction to make legal access, or makes or causes to make illegal access to any computer or computer network or internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or (b) creates pollution or inserts malware in any digital device which may cause or likely to cause death or serious injury to a person; or (c) affects or damages the supply and service of daily commodity of public or creates adverse effect on any critical information infrastructure; or (d) intentionally or knowingly gains access to, or makes interference with, any computer, computer network, internet network, any protected data-information or computer database, or gains access to any such protected data information or computer database which may be used against friendly relations with another foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group, then the act of such person shall be cyber terrorism.'

6. STATE-SANCTIONED LAWFARE: ONGOING CASES UNDER REPEALED LAWS

Apart from the retention of repressive provisions from Section 57 of the ICT Act and DSA in the CSA, lawyers, and defendants who Amnesty International spoke to emphasised that another way these repealed laws continue to live on is through the thousands of cases filed under them, many of which remain ongoing. As noted in the second section of this briefing, 1,271 people were reported to have been charged under Section 57 of the ICT Act before its repeal in 2018, while over 7,000 people were reported to have been charged under DSA before its repeal in 2023.[98] Due to the protracted trial process in Bangladesh, cases filed under Section 57 of the ICT Act continue to haunt those charged under it, even six years after its repeal. This is because when the DSA repealed Section 57 of the ICT Act, the 'repeals and savings clause' still allowed cases filed under Section 57 to 'continue as if the said sections had not been repealed', so long as the case was 'pending at any stage of trial'.[99] The repeal and savings clause in the CSA is even broader since it allows any and all cases filed under DSA to continue even if the investigation or trial process has not commenced.[100] As such, the state has been able to continue framing charges under the DSA against individuals as recently as 28 April 2024, several months after the repeal of

[98] Dhaka Tribune, "Law minister: Over 7,000 cases under DSA", 05 June 2023, https://www.dhakatribune.com/bangladesh/284852/law-minister-over-7-000-cases-under-dsa
[99] DSA, Section 61(2).
[100] CSA, Section 59(2).

the DSA.[101] In February 2024, the Cyber Tribunal in the north-western city of Rangpur sent the editor of a local newspaper to prison after his application for bail was denied during a court hearing for a case filed against him under the DSA.[102]

As one defendant in an ICT Act case explained:

> **"On the one hand the state says the ICT Act and DSA are gone, but on the other hand they are not sparing anyone against whom a case had been filed under these laws. For us, these laws never ceased to exist, and their draconian provisions continue to plague our lives. We continue to face the full brunt of state-sanctioned legal harassment."**

Another senior lawyer representing a defendant in an ICT Act case said, "my client is stuck in a limbo. Like so many others sued under Section 57 for speech offences, he is fed up with having an ICT Act case hanging over his head and having to physically appear in court every six weeks. As the defendant you must show up even if the court date is for submission of the police's investigation report which they keep on delaying. But I suppose attending endless court hearings is still better than being thrown into prison again."

The compulsion to attend court hearings even when the defendant's presence is not required for the fulfillment of the proceedings before the court on that date, is 'targeted harassment', explained the lawyer, since 'the state wants them to be on the run'. For some defendants, several cases were filed under ICT Act or DSA in different districts with concurrent proceedings to exacerbate the costs and hardships of attending multiple court hearings before tribunals located several hours apart from one another.[103] Amnesty International spoke to one such journalist whose life and career continues to be gravely impacted by a case filed under Section 57 of the ICT Act. At the time, he was working for an online news portal where he published an article about a high-ranking government official. This caused a law enforcement agency to file a case against him under Section 57 and then arrest him.

After initially being imprisoned for a week, he was released on bail. However, since the online news portal was subsequently forced to shut down, he became unemployed. Despite having extensive experience in journalism, and being a published author, he felt that he was turned away by every media outlet he applied to, due to the pending ICT case against him. 'No one wanted to be associated with me', he explained to Amnesty International. As such, he stopped writing completely and deactivated all his social media profiles. After facing a multitude of rejections and making vigorous attempts he finally found employment as a news editor at a cable television channel where he shifted his focus away from reporting on political issues. He was slowly rebuilding his life and career. However, after about two years, he was terminated from his employment. He explained that it was due to pressure exerted by the authorities over the outlet for employing an 'anti-state propagandist'. Since then, he has remained unemployed, and living on the verge of economic destitution:

"I have a wife and child to feed but I have no money. It has been almost 2 years that I am jobless. My kid needs milk, but I have no money. If you are in jail, at least they feed you. But if you have no job, then who feeds you?"

He explained how this case has not only disrupted his life and career, but also worsened his health:

"Running after this case has caused me such stress and anxiety that I now have high blood pressure. I need medical check-up which costs upwards of 25,000 BDT. Where will I get that money? Why is the government launching this torture on me? We all know that the court is directed by the government. If the government wants, then tomorrow the case will be dismissed. On the other hand, if they want then tomorrow, I can lose my bail or

[101] New Age, "Online activist Pinaki, ex-JCD leader Ashik charged in DSA case", 28 April 2024, https://www.newagebd.net/post/country/233832/charges-pressed-against-online-activist-pinaki-ex-jcd-leader-ashik-in-dsa-case
[102] Prothom Alo, 'রংপুরে ডিজিটাল নিরাপত্তা আইনের মামলায় সাংবাদিক কারাগারে' ["Journalist in jail in Rangpur Digital Security Act case"], 4 February 2024, https://www.prothomalo.com/bangladesh/district/kl13f7e3gr
[103] Interview by video call with a Senior Advocate of the Supreme Court of Bangladesh (name withheld for security reasons), 3 May 2024.

even face a verdict which will sentence me to lengthy imprisonment. This is our situation. This is our reality. I do not know how much longer I can live like this."

All stakeholders noted how very few escape the state-sanctioned lawfare once it is launched against them. One notable example of a case where the victim of such lawfare was 'fortunate' enough to escape after a lengthy ordeal is university student Khadijatul Kubra. In November 2020, Khadija was a 17-year-old student of political science at Jagannath University when she had hosted a webinar on campus politics for the social media page called 'Humanity for Bangladesh'.[104] Almost two years later, on 27 August 2022, Khadija was arrested under the DSA when the police arrived at her home late at night and then sent her to Kashimpur Jail the next day. Police officers had seen a recording of the webinar on YouTube uploaded by one of the guest speakers – formerly a Bangladeshi army official now based in Canada who had made comments perceived to be critical of the Bangladeshi authorities. They filed two cases under DSA against Khadija and the guest speaker for attempting to 'deteriorate law and order' and for 'defaming' the prime minister, among other charges. Since then, Khadija's bail applications were rejected several times and despite having allegedly developed medical problems including kidney issues, Khadija was transferred to a 'condemned cell' which is reserved for prisoners on death-row.[105]

A family member of Khadija who spoke to Amnesty International in August 2023, when Khadija was still imprisoned, had said:

"When we came to know our Khadija had to spend almost a week in a condemned cell with death row prisoners who are accused of the most serious crimes such as murder, that too during the holy month of Ramadan, we could not eat or sleep for four days. Why is the state punishing her so cruelly? What crime did she commit to warrant this treatment? Last time I visited her, I could see that her eyes were all puffy, as it becomes if one cries all night. Khadija said to me: 'I cannot take it anymore. I cannot live here anymore. I am so afraid. I wish things would go back to normal."

Amnesty International, along with other national and international organisations and human rights defenders, campaigned for the release of Khadija.[106] After spending 14 months in pre-trial detention, she was finally released on bail in November 2023 and then discharged from the DSA cases against her as the cyber tribunal could find no grounds to charge her.[107] One journalist referred to Khadija's case to underscore the lack of accountability and reparation for arbitrary deprivations of liberty:

> **"All the people who were imprisoned arbitrarily under the DSA like Khadija have lost months and years of their lives which they will never get back. They suffered which they will never forget. Yet has the state paid them a penny in compensation?"**

Article 9(5) of the ICCPR requires states' parties to ensure that every person who has been the victim of unlawful arrest or detention has an enforceable right to reparation, including compensation.[108] Forms of reparation include but are not limited to: restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition.[109] In cases of unlawful detention, reparation includes release. Due to the

[104] New Age, "Humanity for Bangladesh holds webinar on campus politics", 13 September 2020 https://www.newagebd.net/article/116048/humanity-for-bangladesh-holds-webinar-on-campus-politics
[105] The Daily Star, "Sued under DSA: JnU student moved to condemned cell for misbehaviour", 24 March 2024, https://www.thedailystar.net/news/bangladesh/crime-justice/news/sued-under-dsa-jnu-student-moved-condemned-cell-misbehaviour-3279091
[106] Amnesty International, "Bangladesh: Authorities must immediately release university student Khadijatul Kubra", 28 August, 2023 https://www.amnesty.org/en/latest/news/2023/08/bangladesh-authorities-must-immediately-release-university-student-khadijatul-kubra/
[107] Dhaka Tribune, "JnU student Khadija discharged from another DSA case", 29 February 2024, https://www.dhakatribune.com/bangladesh/court/340618/jnu-student-khadija-discharged-from-another-dsa; Dhaka Tribune, "JnU student Khadija discharged from one DSA case", 28 January 2024, https://www.dhakatribune.com/bangladesh/court/338014/jnu-student-khadija-discharged-from-one-dsa-case
[108] Although the French and Spanish texts of the ICCPR use the broader term reparation; the term compensation used in the English text is an element of reparation. See: Amnesty International, *Fair Trial Manual – Second Edition*, April 9, 2014 (Index Number: POL 30/002/2014,) p. 68, https://www.amnesty.org/en/documents/POL30/002/2014/en/
[109] Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, UN General Assembly resolution 60/147, Article 18, https://www.ohchr.org/en/instruments-mechanisms/instruments/basic-principles-and-guidelines-right-remedy-and-reparation

underdevelopment of tort law in Bangladesh, victims of rights violations, including victims of unlawful arrest or detention, are seldom able to sue for compensation or other remedies.[110] Against this backdrop, the Supreme Court of Bangladesh has recognised compensation as a remedy for violations of constitutionally guaranteed fundamental rights such as the right to life and liberty. It has held in a number of cases that those arbitrarily arrested and detained by the state have a right to be compensated.[111] As the Government of Bangladesh noted in its first report to the UN Committee against Torture, the Supreme Court has 'awarded compensation for detention of citizens without any legal basis or because of utter negligence'.[112] In 2020, the Supreme Court ordered the state to pay 2 million BDT (USD 17,024) as compensation for the for wrongful arrest and detention of a man who was imprisoned for over five years after police mistook him for an absconding convict.[113] However, these decisions by the court have so far only related to those who were detained due to the negligence of state authorities, so it is unclear whether those held in lengthy pretrial detention under repressive laws, like Khadija, could be awarded compensation by the court.

[110] Taqbir Huda, "Bangladesh: A Constitutional Solution for a Tort Law Deficit?" in Ekaterina Aristova and Ugljesa Grusic (eds), Civil Remedies and Human Rights in Flux: Key Legal Developments in Selected Jurisdictions (Hart Publishing, 2022).
[111] Taqbir Huda, *Civil Liability for Human Rights Violations: A Handbook for Practitioners I Bangladesh,* Bonavero Institute of Human Rights, University of Oxford (2022), https://www.law.ox.ac.uk/sites/default/files/2022-10/5._civil_liabilities_for_human_rights_violations_bangladesh.pdf
[112] Government of Bangladesh, *Initial report submitted by Bangladesh under article 19 of the Convention, due in 1999*, 3 October 2019, Un Doc. CAT/C/BGD/1, para 84.
[113] *Banu v Bangladesh*, Writ Petition No. 7297 of 2019, Supreme Court of Bangladesh, https://supremecourt.gov.bd/resources/documents/1638236_WP_7297_of_2019_2.pdf

7. CASES UNDER THE CSA

Due to the lack of publicly available official data in Bangladesh, it is difficult to estimate the frequency with which the CSA is being used. In the absence of official data, NGOs typically provide unofficial estimates on the number of CSA cases filed which are primarily based on news reports.[114] This reliance on news sources holds true for statistics on human rights violations in Bangladesh more generally.[115] Nevertheless, the Centre for Governance Studies (CGS), a thinktank based in Dhaka, has estimated that at least 61 cases have been filed under CSA accusing 372 individuals, since its enactment on 18 September 2023 to 7 July 2024.[116] One editor cautioned that it would be wrong to look at the comparatively low case-load under the CSA and conclude that it is different from the DSA or that the freedom of expression has been restored in Bangladesh: '

> **"They have kept the exact same law. Just because a weapon is not being used, doesn't mean it is not there. When they need it, they will use it."**

Earlier, the CGS had also published a database on DSA cases, enlisting 1,436 cases filed against 4,520 individuals and 1,549 arrests.[117] A researcher at CGS told Amnesty International in May 2024 that data about CSA cases is proving to be much more difficult than DSA cases due to the possibility of under-reporting in the press.[118] The journalist and lawyers who Amnesty International spoke to similarly cautioned about the very real risk that CSA cases are being under-reported. One local journalist from the coastal sub-district named Patharghata explained that one key reason for under-reporting of CSA cases, compared to those filed under the DSA, is the shift in case filing practices: "Previously we would come to know whenever a case was filed in the police station. However, now, most cyber cases are being filed in the cyber tribunal directly, with only the knowledge of the complainant and their lawyer. Not even the accused knows. They only come to know two or three months later when it comes to investigation stage. By then the case becomes too stale for the news cycle to report on, unless it relates to a VIP or famous person who has news value themselves." The senior researcher from CGS provided a similar explanation and suspected that CSA cases are being underreported in the news due to inaccessibility of information from court sources, as opposed to police sources.[119]

The local correspondent outlined the difficulties he faced before finally being able to report a CSA case that was filed in his locality. First, he contacted the local police station but got no information or corroboration as the case had been filed in the district level cyber tribunal, where he did not have access. He sought corroboration from the complainant's lawyer who initially refused to provide any

[114] See for example: Odhikar, *Bangladesh Annual Human Rights Report 2023*, (2024), https://www.omct.org/site-resources/legacy/Odhikar-Annual-Report-2023.pdf; Odhikar, *Quarterly Human Rights Report (January to March 2024)*.
[115] See for example: Ain o Salish Kendra, Statistics on Human Rights Violations, https://www.askbd.org/ask/statistics-on-human-rights-violations/
[116] Centre for Governance Studies, CSA Tracker, https://csa.freedominfo.net
[117] Centre for Governance Studies, DSA Tracker, https://dsa.freedominfo.net;
[118] Interview over a video call with a researcher from Centre for Governance Studies (name withheld for security reasons), 17 May 2024.
[119] Interview over a video call with a researcher from Centre for Governance Studies (name withheld for security reasons), 17 May 2024.

comment. Only after much convincing and assurance that the report would not did he finally agree. Drawing on this experience, he inquired: "If I could not confirm it, then the newspaper would not even be able to publish it. How many local journalists are going to go through these extra hoops to report on a cyber case that has been filed? At the same time, the only reason I heard about the case being filed is because the complainant and defendant were from the same locality, so word spread when the former went to the tribunal to file a case. However, this may usually not be the case."

Despite the official data gap and likelihood of underreporting, there are several instances where CSA cases have been filed against individuals for allegedly defaming the prime minister or other high ranking government officials on social media.

The earliest such instance is from September 2023, shortly after the CSA was enacted, whereby a case was filed against three individuals before the cyber tribunal in the north-eastern city of Sylhet. They had allegedly been spreading propaganda against the government and uploading distorted photos of the prime minister Sheikh Hasina on Facebook.[120] In October 2023, a similar case was filed in the cyber tribunal of the north-western city of Rangpur against a man for allegedly making defamatory posts about the prime minister and the general secretary of the ruling party on Facebook.[121] In the same month, a young man was arrested from the north-western Nilphamari district for similarly posting distorted photos of the prime minister and the ruling party's general secretary and writing offensive words about them on Facebook.[122] In December 2023, the managing director of a company was arrested in Dhaka for allegedly insulting the state and the prime minister on social media and then sent to rehab as the police suspected he may be 'mentally unbalanced'.[123] In January 2024, a court ordered him to be sent to prison.[124] After his bail was initially denied, he was released on bail in April 2024.[125] In February 2024, a case was filed before the cyber tribunal in Sylhet against a blogger living in exile in Paris, along with several other individuals living in Bangladesh, for publishing distorted photos of the prime minister on social media.[126] In May 2024, a CSA case was filed before the Sylhet Cyber Tribunal against six people for allegedly publishing insulting and satirical pictures of the prime minister on social media.[127] On 4 June 2024, a CSA case was filed before the Sylhet Cyber Tribunal accusing 11 people of insulting and distorting the photos of senior state officials, including the Prime Minister, on Facebook.[128] On 19 June 2024, a man had reportedly been arrested after a case was filed against him under the CSA over a Facebook post where he allegedly mocked the government's quota system for freedom fighters and their families.[129] Three cases are analysed in depth below to further illustrate the way in which the CSA is being used to curtail freedom of expression.

[120] New Age, "Three sued under CSA", 21 September 2023, https://www.newagebd.net/article/212742/three-sued-under-csa
[121] New Age, "US expatriate sued under CSA for remark on PM", 8 October 2023, https://www.newagebd.net/article/214419/us-expatriate-sued-under-csa-for-remark-on-pm
[122] Prothom Alo, "Offensive post on PM, youth arrested in Nilphamari", 6 October 2024, https://www.prothomalo.com/bangladesh/district/neo4s2y9hh
[123] Dhaka Tribune, "Adam Tamizi arrested despite ASK", 10 December 2023, https://www.dhakatribune.com/bangladesh/people/333541/adam-tamizi-arrested-despite-asking-pm-s
[124] The Business Standard, "Adam Tamizi Haque sent to jail in CSA case", 4 January 2024, https://www.tbsnews.net/bangladesh/court/adam-tamizi-haque-sent-jail-csa-case-769530
[125] Dhaka Tribune, "Adam Tamizi Haque gets bail in CSA case", 4 April 2024, https://www.dhakatribune.com/bangladesh/court/343440/adam-tamizi-haque-gets-bail-in-csa-case
[126] Dhaka Tribune, "Pinaki Bhattacharya sued under Cyber Security Act", 18 February 2024, https://www.dhakatribune.com/bangladesh/court/339762/pinaki-bhattacharya-sued-under-cyber-security-act
[127] The Daily New Nation, "6 sued under Cyber Law for insulting Bangabandhu, PM", 8 May 2024, https://thedailynewnation.com/6-sued-under-cyber-law-for-insulting-bangabandhu-pm/
[128] United News of Bangladesh, "11 sued for 'derogatory remarks' against PM in Sylhet", 8 June 2024, https://unb.com.bd/category/Bangladesh/11-sued-for-derogatory-remarks-against-pm-in-sylhet/137113
[129] United News of Bangladesh, "Mocking freedom fighter quota: Man arrested for Facebook post", 20 June 2024, https://unb.com.bd/category/Bangladesh/mocking-freedom-fighter-quota-man-arrested-for-facebook-post/137699

SELIM KHAN

On 4 November 2023, the Bangladeshi police arrested Selim Khan, an atheist blogger for a comment he made on a post in a private Facebook group. According to the First Information Report (FIR) filed with the police, another member of that group took screenshots of Selim's comment and posted it publicly on Facebook with the caption 'How is an atheist moving around by hurting religious sentiment? I wish this son of bitch receives a massive beating'. This public post then went viral on Facebook, causing mass agitation in Selim's town and caused an angry mob to gather outside Selim's house. Selim had left his house for safety, and the police had dispersed the crowd. A local politician (who is also a member of the ruling party) from the same area also saw the screenshot on Facebook and filed a case against Selim under four of the five sweeping speech crimes under the CSA i.e. Sections 25 (offensive information), 28 (hurting religious sentiments), 29 (defamation) and 31 (deteriorating law and order) as well as under Section 153 of the Penal Code which pertains to want only giving provocation and causing riots.

The FIR refers to Selim's blog where he expresses views critical of religion and that people in his village know him to be an atheist antagonistic towards Islam. Selim's lawyer told Amnesty International that the individual who posted Selim's comment publicly on Facebook had joined the private Facebook group to take a screenshot of Selim's posts to specifically target him. Despite being charged with offences which are now all bailable under the CSA, his bail applications were rejected twice, first by the Judicial Magistrate's Court and then by the Court of Sessions. Selim's lawyer explained that he tried and failed to make the judges in the lower courts understand that the offences Selim had been charged with are no longer non-bailable as they were under the DSA. He then petitioned the High Court Division of the Supreme Court of Bangladesh, and after several hearing dates, the appellate court finally granted Selim bail on 13 March 2024. However, when granting bail, the Supreme Court judge commented that hurting religious sentiments should be made a non-bailable offence as it was under the DSA and that it should warrant the highest punishment, such as life imprisonment or even the death sentence.[130] Despite over two months elapsing since Selim was granted bail by the Supreme Court, he has remained in prison as of 23 June 2024. This is because jail officials cannot release prisoners unless the order of bail is communicated in writing from the bail granting court. Selim's lawyer believes that there is a deliberate delay in communicating the bail order to the jail authorities to extend Selim's pre-trial detention, since this process does not usually take more than two weeks to be completed but is taking exceptionally long in his case.

[130] Dhaka Tribune, "HC recommends non-bailable clause for hurting religious sentiments", 13 March 2024, https://www.dhakatribune.com/bangladesh/court/341687/hc-recommends-non-bailable-clause-for-hurting,

SHAMIM ASHRAF

On 18 February 2024, police arrested a cartoonist and activist Shamim Ashraf from his studio in the northern city of Mymensingh. Shamim had designed some posters in the lead up to the Mymensingh City Corporation elections which were critical of the current mayor, who is affiliated with the ruling party. Prior to being arrested by the police, several supporters of the mayor, who were also members of bodies affiliated with the ruling party, barged into Shamim's office, and violently threatened him. This included the mayor's elder brother, who demanded to know who 'made' Shamim design those posters. Some of the posters that the mayor's supporters objected to were designed by Shamim for a climate activist group he is part of, while some were designed for a client, who was another member of the ruling party contesting against the current mayor in the upcoming elections. Shamim Ashraf told Amnesty International: **"Many of the supporters issued violent threats to me from the background, shouting 'we will chop off your head, hands and legs', 'we will shut down your business' and 'we will beat you to death as soon as you step out, can anyone save you?'."** They live-streamed the confrontation on Facebook, which caused news of the incident to spread in the locality. Shamim's client, and the competing mayoral candidate, showed up at the scene with his own set of supporters and tried to mediate the matter but their arrival led to a confrontation between both groups. Shamim found himself caught in a rift between two rival candidates from the ruling party. The police arrived to quell the commotion and then handcuffed Shamim, seized his computers and took him to the police station. Shamim had no scope to ask the police why he was being arrested or why his devices were being seized.

After taking Shamim to the station, the police officers realized that the offences under the CSA they wished to allege against Shamim were no longer cognizable and therefore the CSA case could not be directly filed at the police station or allow Shamim to be arrested without a court warrant. As a result, they resorted to their powers under Section 54 of the Code of Criminal Procedure to justify his arrest, a colonial provision that allows the police widespread powers to arrest individuals without warrants under nine situations, such as when there is reasonable suspicion of a cognizable offence being committed. After spending two nights in jail, Shamim was released on bail. The day he was released on bail, an administrative officer filed a CSA case against Shamim before the cyber tribunal under several sections including Section 25 (false and offensive information), 27 (cyber terrorism) and 29 (defamation). The complaint alleged that Shamim spread 'information terrorism and misinformation in society' which 'created confusion in the minds of the people in the name of City Corporation'. It further stated 'the responsible people of the City Corporation' searched Shamim's studio in the presence of the police, ordinary citizens and witnesses, and obtained the design of the posters with the City Corporation logo from his computer device. It further stated that the accused 'admitted the incident' and this was 'submitted in the learned court in the form of video'. While Shamim remains out on bail, his seized devices are yet to be returned by the police and he continues to face prosecution under the CSA. Shamim told Amnesty International: **"I had four computers in my studio – they seized all four. These are very old computers which I bought back in 2010. They have 14 years' worth of work and my client's data and designs that accumulated over the years. Whenever I ask the police about getting back my devices, they tell me it has been sent to the CID's forensic lab which has a long serial since cases from all over the country come to them. Without my devices it is becoming extremely difficult for me to maintain my graphic design business. At the same time, due to the CSA case filed against me, many clients or partners no longer want to be associated with my studio."**

AKRAMUZZAMAN BIN ABDUS SALAM

In February 2024, a case was filed against Akramuzzaman Bin Abdus Salam, a conservative Islamic preacher under Sections 28 (hurting religious sentiments) and 31 (deteriorating law and order) of the CSA in connection with a video he posted on Facebook. In the video, Abdussalam preached that is far better to visit a brothel than praying on Shab-e-Barat, a night which many Muslims consider to have special spiritual significance. The case alleged that Abdussalam's remarks hurt religious sentiments and disrupted communal harmony and was filed by a member of Ahle Sunnat Wal Jama'at, an Islamic revivalist group. A person closely affiliated with Abdussalam told Amnesty International in May 2024: **"Our laws guarantee religious independence on the one hand and then also limit religion in the name of hurting religious sentiments. People use it as a weapon against those whose religious interpretations go against their own."**

Shaykh Abdussalam promptly published a follow up video apologizing for what he said, stating that he could have worded his critique better. "So, what was the point of this case? The purpose is just to harass. It was filed by those who have long had grievances against our group. We never thought of using the cyber law against them, but they have set an example so maybe in the future cases may be filed against them as well."

8. A STATE OF SELF CENSORSHIP

All journalists and human rights defenders interviewed by Amnesty International invariably described a state of self-censorship that has been catalysed by the systematic use of the DSA. One news editor explained: "The authorities have not needed to use the CSA as frequently as the DSA because we have become very good at toeing the line. We know what can and cannot be said. The line of acceptable speech has been made very clear through many examples before our eyes. Any time someone crossed it, they paid the price. They were punished and harassed. So, we have learned to censor ourselves." She went on to explain that previously, self-censorship existed only at the institutional level. The media outlet would choose to censor a sensitive story the journalist wanted to report on. However, now self-censorship is becoming increasingly common at an individual level, whereby journalists will not even pitch (let alone produce) a sensitive story to their media outlet:

"The culture of self-censorship has trickled down to the lowest levels of reporting. I have been in the media industry for 20 years and I have never seen anything like this. From the most senior journalist to a small fry Youtuber, everyone, and I mean everyone, is now in a state of self-censorship because no one, and I mean no one, can afford to pay the price of speaking up. I mean look at how apprehensive I am about removing any possible identifiable information about myself from the quotes you are going to use from me. That says all you need to know about the freedom of expression in Bangladesh."

Another senior investigative journalist based in Dhaka described how the lawfare launched against those under the DSA has produced a deep-seated climate of fear that has relegated him and other critical voices into silence:

"When you are inside the horrendous and unliveable prisons in our country, you have to pay at least 1,000 BDT a day to stay in there with some level of dignity. When you are released on bail, you are going to have go to court every month to attend the hearing and pay for a lawyer to represent you and handle all the legal hassles. We journalists live hand-to-mouth. So, filing a cyber case against us is a sure-fire way of making us destitute. The level of harassment they can unleash on you for daring to speak truth to power is indescribable. Not even the media outlet you worked for would dare to stand beside you. So which journalist in their right mind would want to take the risk? The risk of losing their job? The risk of losing their family? The risk of losing it all? Self-censorship has become an obligation not only to save yourself, but to save your own family."

A local correspondent for a major national newspaper who is based in the coastal southern city of Barisal described to Amnesty International in May 2024 a turn to self-censorship in similar terms as the journalist from Dhaka: "We are routinely threatened that if we report any news on corruption, we will face a cyber case. Now whenever I see an incident of corruption or abuse of power, I have learned to turn a blind eye. It is too risky. Instead, I stick to positive news about economic growth and development.

However, I cannot write about the millions in public funding that is being misappropriated within these development projects due to corruption." A senior human rights defender had a similar explanation: "since people have imposed self-censorship, most objectionable truths lie hidden." When asked whether she sees a way out of this state of self-censorship, the news editor responded:

> **"The future looks bleak, but the fight must go on. If we never rebelled, then we could never have escaped British colonial rule. But the question is: who will rebel against our current rulers?"**

9. CONCLUSION AND RECOMMENDATIONS

The CSA is essentially a replication of the DSA and continues to threaten the rights to freedom of expression, liberty and privacy in Bangladesh. It does so by rehashing the five authoritarian speech offences, and the sweeping powers of authorities to search, arrest and detain individuals, seize their devices, and block or remove data from the cyber space. The state's persistent lawfare against dissent in the past decade using the DSA and Section 57 of the ICT Act has bulldozed journalists, human rights defenders, activists and critics into a state of self-censorship which will continue to exist unless the repressive features retained in CSA are removed. When enacting the CSA to replace the DSA, the Government of Bangladesh has failed to incorporate (in whole or in part) all but one of the legislative recommendations propounded by the OHCHR. The CSA repackages repression not only by reproducing authoritarian provisions of the DSA, but also through a broadly worded savings clause which allows any case filed under the DSA to continue. In this manner, oppressive laws like the ICT Act and DSA enjoy an afterlife as it continues to haunt the lives of dissidents who were caught within its remit, even several years after their repeal. Bangladesh's continuing lawfare against freedom of expression exemplifies how national and international advocacy efforts aimed at the repeal of a singular piece of legislation will render limited result if underlying authoritarian provisions and practices remain unchanged. In line with our concerns outlined above, Amnesty International urges Bangladesh's authorities to:

Respect, protect, promote and fulfil the human rights of everyone in the country including the rights to freedom of expression, association, and peaceful assembly:

- Immediately and unconditionally release all those detained under the ICT Act, DSA, CSA or any other law solely for peacefully exercising their human rights;
- Expunge the criminal records of all those convicted under the ICT Act, DSA, CSA or any other law simply for the peaceful exercise of their human rights including the right to freedom of expression;
- Ensure that all those released are able to effectively access their right to an effective remedy in accordance with international human rights law, and that they are provided with adequate reparations;
- End the practice of arresting without warrants and bringing criminal charges against those who have simply exercised their human rights including the right to freedom of expression;
- Ensure law enforcement officials who commit violations against individuals are brought to justice in line with international standards of fairness;
- Ensure that all individuals who have been arrested or detained are promptly charged with an internationally recognizable criminal offence or else released and have access to legal counsel of their choice from the outset of their detention, as required by international human rights standards; and
- Ensure that all detainees and prisoners are provided with access to adequate medical care at all times in accordance with international human rights standards, and that prisoners are offered an independent medical examination as soon as possible after admission to a place of detention;

Bring all existing legislation in line with national and international human rights standards:

- Repeal or review and amend all laws that violate the human rights, including the rights to freedom of expression, peaceful assembly and association. In particular: the CSA and provisions of the Penal Code on sedition and defamation, to fully comply with international human rights law, such as the ICCPR, to which Bangladesh is a state party;
- Repeal sections 21, 25 and 28 of the CSA which criminalise legitimate expression of opinions or thoughts and have been used to stifle peaceful dissent under the DSA;
- Repeal Section 31 of the CSA or amend it so it only criminalises speech which clearly constitutes incitement to commit violence or advocated hatred for a specific group, in line with the narrow exceptions to the right to freedom of expression under Article 19 of the ICCPR;
- Fully decriminalise defamation so that it is not subject to any criminal sanction such as fine or imprisonment for default in paying fine as under Section 29 of the CSA and Chapter XXI of the Penal Code 1860. Defamation should exclusively remain a matter of civil law and civil litigation;
- Amend provisions which allow overbroad powers of confiscation, arrest, search, and seizure, such as Sections 40 and 42 of the CSA, so such powers are clearly and narrowly defined. All investigative powers under the law must be subject to safeguards and judicial oversight in line with international human rights law;
- Remove all overbroad, ambiguous, and vague terms from the CSA or provide sufficiently precise terminology that meets the test of legality, consistent with international human rights law;
- Take all the necessary legislative, administrative and other measures, including effective human rights training for judges, prosecutors and other officials, to ensure that the conduct of all criminal proceedings complies fully with international standards with regard to fair trials;
- Introduce legislation expressly granting anyone who has been the victim of unlawful arrest or detention to have an enforceable right to effective remedies, including adequate compensation as stipulated in Article 9(5) of the ICCPR.
- Ratify the First Optional Protocol to the ICCPR to enable individuals to submit complaints to the Human Rights Committee of violations of their rights set out in the Covenant.
- Accede to the Budapest Convention on Cybercrime in line with the procedure set out in Article 37 of the Convention.

Ensure constructive engagement with civil society:

- Extend an invitation to the UN Special Rapporteur on the rights to freedom of opinion and expression to carry out a fact-finding visit to Bangladesh. The Rapporteur should be granted free and unimpeded access to all parts of the country, and freedom to meet with a wide range of stakeholders, including political detainees and prisoners, their families and representatives, in addition to government officials, law enforcement officers and judicial officials.
- Hold public consultations, including with members of the press and civil society, in drafting any new legislation, amendments and/or policy related to cyber space, before they are approved by the cabinet or passed in parliament. Allow sufficient time and scope for members of civil society to provide feedback, and ensure these consultations are inclusive of different groups and are not a mere tick-box exercise as they were with the drafting of the CSA, but are receptive to their feedback and input.

ANNEX 1: COMPARISON OF DIGITAL SECURITY ACT 2018 AND THE CYBER SECURITY ACT 2023

DSA (Official English Translation)	CSA (Unofficial Internal English Translation)	Analysis
1. Short title and commencement. (1) This Act may be called the Digital Security Act, 2018. (2) It shall come into force at once.	**1.** Short title and commencement. (1) This Act may be called the Cyber Security Act, 2023 (2) It shall come into force at once.	Verbatim except change in the title of the law.
2. Definitions. (1) In this Act, unless there is anything repugnant in the subject or context (a) "Appellate Tribunal" means the Cyber Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); (b) "data storage" means information, knowledge, event, basic concept or guideline presented as text, image, audio or video format which (i) is being or has been processed by any computer or computer system or computer network in a formal way; and (ii) has been processed for use in any computer or computer system or computer network; (c) "Agency" means the Digital Security Agency established under section 5 of this Act; (d) "Computer Emergency Response Team" means the National Computer Emergency Response Team or Computer Emergency Response Team formed under section 9; (e) "computer system" means a process interconnected with one or more computers or digital devices capable of collecting, sending and storing information singly or being connected with each other; (f) "Council" means the National Digital Security Council constituted under section 12; (g) "critical information infrastructure" means any external or virtual information infrastructure declared by the Government that controls, processes, circulates or preserves any information-data or electronic information and, if damaged or critically affected, may adversely affect: (i) public safety or financial security or public health, (ii) national security or national integrity or sovereignty; (h) "Tribunal" means the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); (i) "digital" means a working method based on double digit (0 and 1/binary) or digit, and, for carrying out the purposes of this Act, also includes electrical, digital, magnetic, optional, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology; (j) "digital device" means any electronic, digital, magnetic, optical, or information processing device or system which performs logical, mathematical and memory functions by using electronic, digital, magnetic or optical impulse, and is connected with any digital or computer device system or computer network, and also includes all kinds of input, output, processing, accumulation, digital device software or communication facilities; (k) "digital security" means the security of any digital device or digital system;	**2.** Definitions. (1) In this Act, unless there is anything repugnant in the subject or context- (a) "Appellate Tribunal" means the Cyber Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); (b) "data storage" means information, knowledge, event, basic concept or guideline presented as text, image, audio, or video format which: (i) is being or has been processed by any computer or computer system or computer network in a formal way; and (ii) has been processed for use in any computer or computer system or computer network; (c) "Agency" means the Cyber Security Agency established under section 5 of this Act; (d) "Computer Emergency Response Team" or "Computer Incident Response Team" means the Computer Emergency Response Team or Computer Incident Response Team described in sub-section (2) of section 9; (e) "computer system" means a process interconnected with one or more computers or digital devices capable of collecting, sending, and storing information singly or being connected with each other; (f) "Council" means the National Cyber Security Council constituted under section 12; (g) "Critical Information Infrastruc ture" means any external or virtual information infrastructure declared by the Government that controls, processes, circulates, or preserves any information-data or any digital or electronic information and, if damaged or critically affected, may adversely affect: (i) public safety or financial security or public health, (ii) national security or national integrity or sovereignty; (h) "National Computer Emergency Response Team" means the National Computer Emergency Response Team described in sub-section (1) of section 9; (i) "Tribunal" means the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006); (j) "digital" means a working method based on double-digit (0 and 1/binary) or digit, and, for carrying out the purposes of this Act, also includes electrical, digital, magnetic, optional, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology; (k) "digital device" means any electronic, digital, magnetic, optical, or information processing device or system which performs logical, mathematical, and memory functions by using electronic, digital, magnetic, or optical impulses, and is connected with any digital or computer device system or computer network, and also includes all kinds of input,	Verbatim, except five minor changes: (i) Reference to "Computer Incident Response team" added to the definition of "Computer Emergency Response Team" (ii) Definition of "National Computer Emergency Response Team" introduced (iii) Definition of "digital security" removed (iv) Reference to electronic device added to definition of "malware" (v) Definition of "cyber security" added (in place of "digital security")

(l) “digital forensic lab” means the digital forensic lab established under section 10;

(m) “police officer” means a police officer not below the rank of a Sub-Inspector;

(n) “programme” means instructions expressed in the form of sound, signal, graph, or in any other form produced with the help of a machine in a readable medium through which any special function can be executed or be made tangibly productive by using digital device;

(o) “Criminal Procedure” means the Code of Criminal Procedure, 1898 (Act V of 1898);

(p) “person” means any person or institution, company, partnership business, farm or any other organization, or in case of the digital device, its controller, and also includes any entity created by law or any artificial legal entity;

(q) “illegal access” means to access into any computer or digital device or digital network or digital information system, without permission of the concerned person or authority or in violation of the conditions of such permission, or by means of such access, to make interruption in exchanging any data-information of such information system, or to suspend or prevent or stop the process of exchanging data-information, or to change or insert or add or deduct the data-information, or to collect any data-information by means of a digital device;

(r) “Director General” means the Director General of the Agency;

(s) “defamation” means defamation as defined under section 499 of the Penal Code (Act XLV of 1860);

(t) “malware” means such kind of computer or digital instruction, data- information, programme or apps which:
(i) changes, distorts, destructs, damages or affects any activity done by digital device or computer, or creates adverse effect on performing activity of it; or
(ii) being connected with any other computer or digital device, becomes auto-active while activating any programme, data- information or instruction of the computer or digital device, doing any function, and by means of which causes harmful changes or incident in the computer or digital device;
(iii) creates opportunity of stealing information from a digital device or automatic access to it;

(u) “spirit of liberation war” means the high ideals of nationalism, socialism, democracy and secularism which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle; and

(v) “service provider” means:
(i) any person who enables any user to communicate through computer or digital process; or
(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.

(2) The words and expressions used in this Act but not defined shall have the same meaning as are used in the Information and Communication Technology Act, 2006.

output, processing, accumulation, digital device software or communication facilities;

(l) “digital forensic lab” means the digital forensic lab established under section 10;

(m) “police officer” means a police officer not below the rank of a Sub-Inspector;

(n) “programme” means instructions expressed in the form of a sound, signal, graph, or in any other form produced with the help of a machine in a readable medium through which any special function can be executed or be made tangibly productive by using a digital device;

(o) “Criminal Procedure” means the Code of Criminal Procedure, 1898 (Act V of 1898);

(p) “person” means any person or institution, company, partnership business, firm, or any other organization, or in the case of the digital device, its controller, and also includes any entity created by law or any artificial legal entity;

(q) “illegal access” means to access any computer or digital device or digital network or digital information system, without permission of the concerned person or authority or in violation of the conditions of such permission, or by means of such access, to make interruption in exchanging any data-information of such information system, or to suspend or prevent or stop the process of exchanging data-information, or to change or insert or add or deduct the data-information, or to collect any data-information by means of a digital device;

(r) “Director General” means the Director General of the Agency;

(s) “defamation” means defamation as defined under section 499 of the Penal Code (Act XLV of 1860);

(t) “malware” means such kind of computer or digital instruction, data information, programme, or apps which:
(i) changes, distorts, destructs, damages, or affects any activity done by digital device or computer, or creates an adverse effect on performing the activity of it; or
(ii) being connected with any other computer or digital device, becomes auto-active while activating any programme, data information, or instruction of the computer or digital device, doing any function, and by means of which causes harmful changes or incident in the computer or digital or electronic device;
(iii) creates an opportunity of stealing information from a digital or electronic device or automatically access it;

(u) “spirit of liberation war” means nationalism, socialism, democracy, and secularism which are the ideals which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle;

(v) “cyber security” means the security of any digital device, computer, or computer system;

(w) “service provider” means:
(i) any person who enables any user to communicate through a computer or digital process; or
(ii) any person, entity, or institution who processes or preserves computer data in favour of the service or the user of the service.

(2) The words and expressions used in this Act but not defined shall have the same meaning as are used in the Information and Communication Technology Act, 2006.

3. Application of the Act. If any provision of any other law is inconsistent with any provision of this Act, the provision of this Act shall apply to the extent inconsistent with the provision of that any other Act: Provided that the provisions of the Right to Information Act, 2009 (Act No. XX of 2009) shall be applicable to a matter related to right to information.	**3.** Application of the Act. (1) If any provision of any other law is inconsistent with any provision of this Act, the provision of this Act shall apply to the extent inconsistent with the provision of that other Act. (2) Notwithstanding anything contained in sub-section (1), the provisions of the Right to Information Act, 2009 (Act No. XX of 2009) shall be applicable to a matter related to the right to information.	Verbatim except formalistic changes.
4. Extra territorial application of the Act. (1) If any person commits any offence under this Act beyond Bangladesh which would be punishable under this Act if committed in Bangladesh, the provisions of this Act shall be applicable in such manner as if he had committed such offence in Bangladesh. (2) If any person commits any offence within Bangladesh under this Act from outside of Bangladesh using any computer, computer system, or computer network situated in Bangladesh, the provisions of this Act shall be applicable to the person in such manner as if the whole process of the offence had been committed in Bangladesh. (3) If any person commits any offence beyond Bangladesh under this Act from inside of Bangladesh, the provisions of this Act shall be applicable in such manner as if the whole process of the offence had been committed in Bangladesh.	**4.** Extraterritorial application of the Act. (1) If any person commits any offence under this Act beyond Bangladesh which would be punishable under this Act if committed in Bangladesh, the provisions of this Act shall be applicable in such manner as if he had committed such offence in Bangladesh. (2) If any person commits any offence within Bangladesh under this Act from outside of Bangladesh using any computer, computer system, or computer network situated in Bangladesh, the provisions of this Act shall be applicable to the person in such manner as if the whole process of the offence had been committed in Bangladesh. (3) If any person commits any offence beyond Bangladesh under this Act from inside of Bangladesh, the provisions of this Act shall be applicable in such manner as if the whole process of the offence had been committed in Bangladesh.	Verbatim.
5. Establishment of Agency, Office, etc. (1) For carrying out the purposes of this Act, the Government shall, by notification in the official Gazette, establish an Agency to be called the Digital Security Agency consisting of 1 (one) Director General and 2 (two) Directors. (2) The head office of the Agency shall be in Dhaka, but the Government may, if necessary, set up its branch offices at any place in the country outside of Dhaka. (3) The powers, responsibilities and functions of the Agency shall be prescribed by rules.	**5.** Establishment of Agency, Office, etc. (1) For carrying out the purposes of this Act, the Government shall, by notification in the official Gazette, establish an Agency to be called the National Cyber Security Agency consisting of 1 (one) Director General and such number of Directors as may be prescribed by the Rule. (2) The head office of the Agency shall be in Dhaka, but the Government may, if necessary, set up its branch offices at any place in the country outside of Dhaka. (3) The Agency shall be administratively attached to the Information and Communication Technology Division as a Department. (4) The powers, responsibilities, and functions of the Agency shall be prescribed by rules.	Verbatim, except addition of one new subsection which stipulates that the Cyber Security Agency will be part of the Information and Communication Technology Division.
6. Appointment of the Director General and the Directors, tenure, etc. (1) The Director General and the Directors shall be appointed by the Government from among the persons specialist in computer or cyber security, and the terms and conditions of their service shall be determined by the Government. (2) The Director General and the Directors shall be full time employees of the Agency and shall, subject to the provisions of this Act and rules made thereunder, perform such functions, exercise such powers and discharge such duties as may be directed by the Government. (3) If a vacancy occurs in the office of the Director General, or if the Director General is unable to perform his duties on account of absence, illness or any other cause, the senior most Director shall provisionally perform the duties of the Director General until the newly appointed Director General assumes his office or the Director General is able to resume the functions of his office.	**6.** Appointment of the Director General and the Directors, tenure, etc. (1) The Director General and the Directors shall be appointed by the Government from among the persons specialist in computer or cyber security, and the terms and conditions of their service shall be determined by the Government. (2) The Director General and the Directors shall be full-time employees of the Agency and shall, subject to the provisions of this Act and rules made thereunder, perform such functions, exercise such powers and discharge such duties as may be directed by the Government. (3) If a vacancy occurs in the office of the Director General, or if the Director General is unable to perform his duties on account of absence, illness or any other cause, the senior most Director shall provisionally perform the duties of the Director General until the newly appointed Director General assumes his office or the Director General is able to resume the functions of his office.	Verbatim.

7. Manpower of the Agency. (1) The Agency shall have necessary manpower according to the organizational framework approved by the Government. (2) The Agency may, subject to such terms and conditions as may be prescribed by rules, appoint such number of employees as may be necessary for the efficient performance of its functions.	**7.** Manpower of the Agency. (1) The Agency shall have the necessary manpower according to the organizational framework approved by the Government. (2) The terms and conditions of employment of the manpower of the Agency shall be determined by Rules.	Verbatim, except minor change in reference to the rules.
8. Power to remove or block some data-information. (1) If any data- information related to any matter under the jurisdiction of the Director General, being published or propagated in digital media, creates threat to digital security, the Director General may request the Bangladesh Telecommunications and Regulatory Commission, hereinafter referred to as BTRC, to remove or, as the case may be, block the said data-information. (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 discipline 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. (3) If BTRC is requested under sub-sections (1) and (2), it shall, with intimation to the Government of the said matters, instantly remove or, as the case may be, block the data-information. (4) For carrying out the purposes of this section, other necessary matters shall be prescribed by rules.	**8.** Power to remove or block some data-information. (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 Regulatory Commission, hereinafter referred to as BTRC, to remove or, as the case may be, block the said data-information. (2) If, subject to the analysis of data by the law and order enforcing force, there is reason to believe that any data-information published or propagated in digital media hampers the solidarity, financial activities, security, defence, religious values or public discipline 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. (3) If BTRC is requested under sub-sections (1) and (2), it shall, with intimation to the Government of the said matters, instantly remove or, as the case may be, block the data information. (4) For carrying out the purposes of this section, other necessary matters shall be prescribed by rules.	Verbatim, except replacing 'digital security' with 'cyber security' and minor change to the wording of Subsection 8(2) which introduces the need for the Director General of the Cyber Security Agency to analyse data and have reasonable belief of harm before requesting it to be removed.
9. Emergency Response Team. (1) For carrying out the purposes of this Act, there shall be a National Computer Emergency Response Team under the Agency, for discharging duties on full time basis. (2) Any critical information infrastructure declared under section 15 may, if necessary, form its own Computer Emergency Response Team, with the prior approval of the Agency. (3) The Computer Emergency Response Team shall consist of the persons expert in digital security and, if necessary, members of law and order enforcing force. (4) The Computer Emergency Response Team shall discharge its duties in such manner as may be prescribed by rules, on full time basis. (5) Without prejudice to the generality of sub-section (4), the Computer Emergency Response Team shall discharge the following duties, namely: (a) to ensure the emergency security of the critical information infrastructure; (b) to take immediate necessary measures for remedy if there is any cyber or digital attack and if the cyber or digital security is affected; or (c) to take necessary initiatives to prevent probable and imminent cyber or digital attack; (d) to take overall co-operational initiatives, including exchange of information with any similar type of foreign team or organization, for carrying out the purposes of this Act, with the prior approval of the Government; and (e) to do such other act as may be prescribed by rules. (6) The Agency shall supervise and make co-ordination among the Computer Emergency Response Teams.	**9. Computer** Emergency Response Team. (1) For carrying out the purposes of this Act, there shall be a National Computer Emergency Response Team under the Agency, for discharging duties on full time basis. (2) Any critical information infrastructure declared under section 15 may, if necessary, form its own Computer Emergency Response Team or Computer Incident Response Team, with the prior approval of the Agency. (3) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall consist of the persons expert in cyber security and, if necessary, members of law and order enforcing force. (4) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge their duties in such manner as may be prescribed by rules, on full time basis. (5) Without prejudice to the generality of sub-section (4), the National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge the following duties, namely: - (a) to ensure the emergency security of the critical information infrastructure; (b) to take immediate necessary measures for remedy if there is any cyber or digital attack and if the cyber or digital security is affected; or (c) to take necessary initiatives to prevent probable and imminent cyber or digital attack; (d) to take overall co-operational initiatives, including exchange of information with any similar type of foreign team or organization, for carrying out the purposes of this Act, with the prior approval of the Government; and (e) to do such other act as may be prescribed by rules. (6) The Agency shall supervise and make co-ordination among the National Computer Emergency Response Team	Verbatim except one minor change (references to the National Computer Emergency Response Team and/or Computer Incident Response Team added).

	and the Computer Emergency Response Team or the Computer Incident Response Teams.	
10. Digital forensic lab. (1) For carrying out the purposes of this Act, there shall be one or more digital forensic labs under the control and supervision of the Agency. (2) Notwithstanding anything contained in sub-section (1), if any digital forensic lab is established under any authority or organisation of the Government before the commencement of this Act, the Agency shall, subject to fulfilment of the standard prescribed under section 11, give recognition to the forensic lab and in such case, the lab shall be deemed to have been established under this Act. (3) The Agency shall make co-ordination among the digital forensic labs. (4) The establishment, use, operation and other matters of the digital forensic lab shall be prescribed by rules.	**10.** Digital forensic lab. (1) For carrying out the purposes of this Act, there shall be one or more digital forensic labs under the control and supervision of the Agency. (2) Notwithstanding anything contained in sub-section (1), if any digital forensic lab is established under any authority or organisation of the Government before the commencement of this Act, the Agency shall, subject to fulfilment of the standard prescribed under section 11, give recognition to the forensic lab and in such case, the lab shall be deemed to have been established under this Act. (3) The Agency shall make co-ordination among the digital forensic labs. (4) The establishment, use, operation, and other matters of the digital forensic lab shall be prescribed by rules.	Verbatim.
11. Quality control of digital forensic lab. (1) The Agency shall ensure the quality of each digital forensic lab, according to the standards prescribed by rules. (2) In case of ensuring the quality prescribed under sub-section (1), each digital forensic lab shall, inter alia, (a) operate the functions of the lab by properly qualified and trained manpower; (b) ensure its physical infrastructural facilities; (c) take necessary initiatives to maintain the security and secrecy of the data-information preserved thereunder; (d) use quality instruments in order to maintain the technical standard of the digital test; and (e) perform its functions following scientific method in such manners as may be prescribed by rules.	**11.** Quality control of digital forensic lab. (1) The Agency shall ensure the quality of each digital forensic lab, according to the standards prescribed by rules. (2) In case of ensuring the quality prescribed under sub-section (1), each digital forensic lab shall, inter alia, - (a) operate the functions of the lab by properly qualified and trained manpower; (b) ensure its physical infrastructural facilities; (c) take necessary initiatives to maintain the security and secrecy of the data information preserved thereunder; (d) use quality instruments in order to maintain the technical standard of the digital forensic test; and (e) perform its functions following the scientific method in such manners as may be prescribed by rules.	Verbatim, except one minor change (reference to digital forensic test added).
12. National Digital Security Council. (1) For carrying out the purposes of this Act, the National Digital Security Council shall consist of a Chairman and the following 13 (thirteen) members, namely: (a) Chairman; (b) Minister, State Minister or Deputy Minister of the Ministry of Post, Telecommunication and Information Technology; (c) Minister, State Minister or Deputy Minister of the Ministry of Law, Justice and Parliamentary Affairs; (d) Principal Secretary to the Prime Minister; (e) Governor, Bangladesh Bank; (f) Secretary, Posts and Telecommunication Division; (g) Secretary, Information and Communication Technology Division; (h) Secretary, Public Security Division; (i) Foreign Secretary, Ministry of Foreign Affairs; (j) Inspector General of Police, Bangladesh Police; (k) Chairman, BTRC; (l) Director General, Directorate General of Forces Intelligence; (m) Director General, Member Secretary. (2) The Prime Minister of the Government of the People's Republic of Bangladesh shall be the Chairman of the Council. (3) For carrying out the purposes of sub-section (1), the Council, in consultation with the Chairman, may, at any time, by notification in the official Gazette, co-opt any specialist as its member, on such terms and conditions as may be prescribed [such as: any specialist on recommendation of the Bangladesh Computer Samity (BCS), Bangladesh Association of Software and Information Services (BASIS), Internet Service Providers Association of Bangladesh (ISPAB), National Telecommunication	**12.** National Cyber Security Council. (1) For carrying out the purposes of this Act, the National Cyber Security Council shall consist of the following members, namely: (a) Prime Minister,o Government of the People's Republic of Bangladesh, who shall be its Chairman; (b) Minister, State Minister or Deputy Minister of the Ministry of Post, Telecommunication and Information Technology; (c) Minister of the Ministry of Law, Justice and Parliamentary Affairs; (d) Advisor of ICT affairs to the Prime Minister (e) Principal Secretary to the Prime Minister; (f) Governor, Bangladesh Bank; (g) Secretary, Posts and Telecommunication Division; (h) Secretary, Information and Communication Technology Division; (i) Secretary, Public Security Division; (j) Foreign Secretary, Ministry of Foreign Affairs; (k) Inspector General of Police, Bangladesh Police; (l) Chairman, Bangladesh Telecommunication Regulatory Commission; (m) Director General, Directorate General of Forces Intelligence; (n) Director General, National Security Intelligence; (o) Director General, National Telecommunication Monitoring Centre; (p) Director General, National Cyber Security Agency (2) The Director General shall provide secretarial assistance to the Council to perform its functions (3) For carrying out the purposes of sub-section (1), the Council, in consultation with the Chairman, may, at any time, by notification in the official Gazette, co-opt any	Verbatim, except three minor changes: (i) the heads of three other executive agencies are added to the membership of the National Cyber Security Council. (ii) a new subsection requiring the Director General to provide secretarial assistance to the Council added. (iii) references to the BCS, BASIS, ISPAB, and NTMC removed from Section 12(3).

Monitoring Centre (NTMC) or 1 (one) representative of mass media on recommendation of Ministry of Information].	specialist as its member, on such terms and conditions as may be prescribed.	
13. Power, etc. of the Council. (1) For implementation of the provisions of this Act and the rules made thereunder, the Council shall provide necessary direction and advice to the Agency. (2) The Council shall, inter alia, perform the following functions, namely: (a) to provide necessary directions for remedy if digital security is under threat; (b) to give advice for infrastructural development of digital security and enhancement of its manpower and quality; (c) to formulate inter-institutional policies to ensure the digital security; (d) to take necessary measures to ensure the proper application of this Act and rules made thereunder; and (e) to do such other act as may be prescribed by rules. (3) The Agency shall provide necessary secretarial assistance to the Council to perform its functions.	**13.** Power, etc. of the Council. (1) For implementation of the provisions of this Act and the rules made thereunder, the Council shall provide necessary direction and advice to the Agency. (2) The Council shall, inter alia, perform the following functions, namely: - (a) to provide necessary directions for remedy if cyber security is under threat; (b) to give advice for infrastructural development of cyber security and enhancement of its manpower and quality; (c) to formulate inter-institutional policies to ensure the cyber security; (d) to take necessary measures to ensure the proper application of this Act and rules made thereunder; and (e) to do such other act as may be prescribed by rules.	Verbatim, except two minor changes: (i) reference to "digital security" replaced with "cyber security". (ii) Section 13(3) removed.
14. Meeting, etc. of the Council. (1) Subject to other provisions of this section, the Council may determine the procedure of its meeting. (2) The meeting of the Council shall be held on such date, time and place as may be determined by its Chairman. (3) The Council shall hold its meetings as and when necessary. (4) The Chairman of the Council shall preside over all meetings of the Council. (5) No act or proceeding of the Council shall be invalid and be called in question merely on the ground of any vacancy in, or any defect in the constitution of, the Council.	**14.** Meeting, etc. of the Council. (1) Subject to other provisions of this section, the Council may determine the procedure of its meeting. (2) The meeting of the Council shall be held on such date, time and place as may be determined by its Chairman. (3) The Chairman may call a meeting of the Council at any time. (4) The Chairman shall preside over all meetings of the Council. (5) No act or proceeding of the Council shall be invalid and be called in question merely on the ground of any vacancy in, or any defect in the constitution of, the Council.	Verbatim.
15. Critical information infrastructure. For carrying the purposes of this Act, the Government may, by notification in the official Gazette, declare any computer system, network or information infrastructure as critical information infrastructure	**15.** Critical information infrastructure. For carrying the purposes of this Act, the Government may, by notification in the official Gazette, declare any computer system, network or information infrastructure as critical information infrastructure.	Verbatim.
16. Monitoring and inspection of the safety of a critical information infrastructure. (1) The Director General shall, if necessary, from time to time, monitor and inspect any critical information infrastructure to ensure whether the provisions of this Act are properly complied with, and submit a report in this behalf to the Government. (2) The critical information infrastructures declared under this Act shall, upon examination and inspection of its internal and external infrastructures, submit an inspection report to the Government every year in such manner as may be prescribed by rules, and communicate the subject matter of the report to the Director General. (3) If the Director General has reason to believe that any activity of an individual regarding any matter within his jurisdiction is threatening or detrimental to any critical information infrastructure, then he may, suo moto, or upon a complaint of any other person, inquire into the matter. (4) For carrying out the purposes of this Act, the inspection and examination of safety of any critical information infrastructure shall be conducted by a person expert in digital security.	**16.** Monitoring and inspection of the safety of a critical information infrastructure. (1) The Director General shall, if necessary, from time to time, monitor and inspect any critical information infrastructure to ensure whether the provisions of this Act are properly complied with, and submit a report in this behalf to the Government. (2) The critical information infrastructures declared under this Act shall, upon examination and inspection of its internal and external infrastructures, submit an inspection report to the Government every year in such manner as may be prescribed by rules, and communicate the subject matter of the report to the Director General. (3) If the Director General has reason to believe that any activity of an individual regarding any matter within his jurisdiction is threatening or detrimental to any critical information infrastructure, then he may, suo moto, or upon a complaint of any other person, inquire into the matter. (4) For carrying out the purposes of this Act, the inspection and examination of safety of any critical information infrastructure shall be conducted by a person expert in cyber security.	Verbatim.
17. Punishment for illegal access to any critical information infrastructure.	**17.** Punishment for illegal access to any critical information infrastructure.	Verbatim, except changes to sentencing. Maximum applicable sentence for the offence under section 17(a)

(1) If any person, (A) intentionally or knowingly, makes illegal access to any critical information infrastructure or (B) by means of illegal access, causes or tires to cause harm or damage to it, or make or tries to make it inactive then such act of the person shall be an offence (2) If any person (A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 25 (twenty-five) lac, or with both; and (B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both	(1) If any person, intentionally or knowingly, (A) makes illegal access to any critical information infrastructure; or (B) by means of illegal access, causes or tries to cause harm or damage to it, or makes or tries to make it inactive, then such act of the person shall be an offence. (2) If any person - (A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Take 25 (twenty-five) lac, or with both; and (B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 6 (six) years, or with fine not exceeding Taka 1 (one) crore, or with both.	reduced by four years. Maximum applicable sentence for the offence under section 17(b) reduced by eight years. Higher punishment applicable to repeat offenders removed.
18. Illegal access to computer, digital device, computer system, etc. and punishment. (1) If any person intentionally (a) makes or abets to make illegal access to any computer, computer system or network or (b) makes or abets to make illegal access with intent to commit an offence, then such act of the person shall be an offence. (2) If any person (A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 6 (six) months, or with fine not exceeding Taka 2 (two) lac, or with both; (B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any offence under sub-section (1) is committed to a protected computer or computer system or computer network, he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (4) If any person commits an offence under this section for the second time or repeatedly, he shall be liable to double of the punishment provided for that offence.	**18.** Illegal access to computer, digital device, computer system, etc. and punishment. (1) If any person intentionally (a) makes or abets to make illegal access to any computer, computer system or computer network; or (b) makes or abets to make illegal access to any computer, digital device, computer system or computer network with intent to commit an offence, then such act of the person shall be an offence. (2) If any person (A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 6 (six) months, or with fine not exceeding Taka 2 (two) lac, or with both; (B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any offence under sub-section (1) is committed to a computer or computer system or computer network protected by critical information infrastructure, he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both.	Verbatim, except addition of reference to 'computer network' in subsection (1)(a), 'any computer, digital device, computer system or computer network' in subsection 1(b) and 'protected by critical information infrastructure' to subsection (3). Higher punishment applicable to repeat offenders under subsection (4) has been removed.
19. Damage of computer, computer system, etc. and punishment. (1) If any person (a) collects any data, data-storage, information or any extract of it from any computer, computer system or computer network, or collects information with moveable stored data-information of such computer, computer system or computer network, or collects copy or extract of any data; or (b) intentionally inserts or tries to insert any virus or malware or harmful software into any computer or computer system or computer network; or (c) willingly causes or tries to cause harm to data or data-storage of any computer, computer system, computer network, or causes or tries to cause harm to any programme saved in the computer, computer system, or computer network; or (d) obstructs or tries to obstruct a valid or authorized person to access into any computer, computer system or computer network by any means; or (e) willingly creates or sells or tries to create or sell spam or sends unsolicited electronic mails without permission of the sender or receiver, for marketing any product or service; or (f) takes service of any person, or deposits or tries to credit the charge fixed for the service to the account of any other person fraudulently or by means of unfair interference to any computer, computer system or computer network,	**19.** Damage of computer, computer system, etc. and punishment. (1) If any person (a) collects any data, data-storage, information or any extract of it from any computer, computer system or computer network, or collects information with moveable stored data-information of such computer, computer system or computer network, or collects copy or extract of any data; or (b) intentionally inserts or tries to insert any virus or malware or harmful software into any computer or computer system or computer network; or (c) willingly causes or tries to cause harm to data or data-storage of any computer, computer system, computer network, or causes or tries to cause harm to any programme saved in the computer, computer system, or computer network; or (d) obstructs or tries to obstruct a valid or authorized person to access into any computer, computer system or computer network by any means; or (e) willingly creates or sells or tries to create or sell spam or sends unsolicited electronic mails without permission of the sender or receiver, for marketing any product or service; or (f) takes service of any person or deposits or tries to credit the charge fixed for the service to the account of any other person fraudulently or by means of unfair interference to any computer, computer system or computer network,	Verbatim except removal of higher punishment applicable to repeat offenders under subsection (3).

then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both.	then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.	
20. Offence and punishment related to modification of computer source code. (1) If any person intentionally or knowingly hides or damages or modifies the source code used in any computer programme, computer system or computer network, or tries to hide, damage or modify the source code, programme, system or network through another person, and if such source code is preservable or maintainable, then such act of the person shall be an offence. (2) If any person commits any offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 3 (three) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.	**20**. Offence and punishment related to modification of computer source code (1) If any person intentionally or knowingly hides or damages or modifies the source code used in any computer programme, computer system or computer network, or tries to hide, damage or modify the source code, programme, system or network through another person, and if such source code is preservable or maintainable, then such act of the person shall be an offence. (2) If any person commits any offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 3 (three) lac, or with both.	Verbatim except removal of higher punishment applicable to repeat offenders under subsection (3).
21. Punishment for making any kind of 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 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. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 1 (one) crore, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine of Taka 3 (three) crore, or with both.	**21.** Punishment for carrying out any hateful, confusing and defamatory campaign about liberation war, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag. (1) If any person, by means of digital or electronic medium, carries out or instigates to carry out any propaganda or campaign against the liberation war of Bangladesh, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 1 (one) crore, or with both.	There are four changes. First, the description of the offence now includes new broad terminologies such as 'hateful', 'confusing' and 'defamatory' and explicit reference to Bangabandhu Sheikh Mujibur Rahman as the father of the nation. Second, reference to 'electronic medium' has been added in subsection (1). Third, maximum applicable sentence for the offence has been reduced by three years. Fourth, higher punishment applicable to repeat offenders under subsection (3) has been removed.
22. Digital or electronic forgery (1) If any person commits forgery by using any digital or electronic medium, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both. Explanation.- For carrying out the purposes of this section, "digital or electronic forgery" means to operate, without right or in excess of the right given or by means of unauthorized practice, erroneous data or programme, information or wrong activity, information system, computer or digital network by	**22**. Digital or electronic forgery (1) If any person commits forgery by using any digital or electronic medium, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 5 (five) lac, or with both. Explanation. - For carrying out the purposes of this section, "digital or electronic forgery" means to operate, without right or in excess of the right given or by means of unauthorized practice, erroneous data or programme, information or wrong activity, information system, computer or digital network by producing, changing, deleting and hiding input or output of any computer or digital device by a person.	Verbatim except two sentencing-related changes. First, the maximum applicable sentence for the offence has been reduced by three years. Second, the higher punishment applicable to repeat offenders has been removed.

producing, changing, deleting and hiding input or output of any computer or digital device by a person.		
23. Digital or electronic fraud (1) If any person commits fraud by using any digital or electronic medium, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both. Explanation. - For carrying out the purposes of this section, "digital or electric fraud" means to change or delete any information of, or add new information to, or tamper any information of, any computer programme, computer system, computer network, digital device, digital system, digital network or social media by a person, intentionally or knowingly or without permission, and doing so, to diminish the value or utility thereof, or try to get any benefit for himself or any other person, or to cause harm to, or deceive, any other person.	**23**. Digital or electronic fraud 1) If any person commits fraud by using any digital or electronic medium, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. Explanation. - For carrying out the purposes of this section, "digital or electric fraud" means to change or delete any information of, or add new information to, or tamper any information of, any computer programme, computer system, computer network, digital device, digital system, digital network or social media by a person, intentionally or knowingly or without permission, and doing so, to diminish the value or utility thereof, or try to get any benefit for himself or any other person, or to cause harm to, or deceive, any other person.	Verbatim, except removal of higher punishment applicable to repeat offenders.
24. Identity fraud or personation (1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network- (a) holds the identity of another person or exhibits the personal information of another person as his own in order to deceive or cheat; or (b) holds the personal identity of any person, alive or dead, as his own by forgery in order to- (i) get or cause to get benefit for himself or for any other person; (ii) acquire any property or any interest therein; (iii) cause harm to a natural person or individual by personating another, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.	**24.** Identity fraud or personation (1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network- (a) holds the identity of another person or exhibits the personal information of another person as his own in order to deceive or cheat; or (b) holds the personal identity of any person, alive or dead, as his own by forgery in order to- (i) get or cause to get benefit for himself or for any other person; (ii) acquire any property or any interest therein; (iii) cause harm to a natural person or individual, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.	Verbatim, except removal of higher punishment applicable to repeat offenders.
25. Transmission, publication, etc. of offensive, false or threatening data- information 1) If any person, through any website or any other digital medium, (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 (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, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 3 (three) lac, or with both.	**25**. Transmission, publication, etc. of offensive, false or threatening data- information (1) If any person, through any website or any other digital medium, (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 (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, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 3 (three) lac, or with both.	Verbatim, except two sentencing related changes. First, the maximum applicable prison sentence for the offence has been reduced by one year. Second, the higher mandatory imprisonment for repeat offenders has been removed.

(3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 5(five) years, or with fine not exceeding Taka 10 (ten) lac, or with both.		
26. Punishment for unauthorized collection, use etc. of identity information. (1) If any person collects, sells, possesses, provides or uses identity information of any other person without lawful authority, then such act of the person shall be an offence. (2) If any person commits any offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both. Explanation. - For carrying out the purposes of this section, "identity information" means any external, biological or physical information or any other information which singly or jointly can identify a person or a system, such as- name, photograph, address, date of birth, mother's name, father's name, signature, national identity card, birth and death registration number, finger print, passport number, bank account number, driving license, e-TIN number, electronic or digital signature, username, credit or debit card number, voice print, retina image, iris image, DNA profile, security related question or any other identification which are available for advance technology.	**26**. Punishment for unauthorized collection, use etc. of identity information. (1) If any person collects, sells, possesses, provides or uses identity information of any other person without lawful authority, then such act of the person shall be an offence. (2) If any person commits any offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 5 (five) lac, or with both. Explanation. - For carrying out the purposes of this section, "identity information" means any external, biological or physical information or any other information which singly or jointly can identify a person or a system, such as- name, photograph, address, date of birth, mother's name, father's name, signature, national identity card, birth and death registration number, finger print, passport number, bank account number, driving license, e-TIN number, electronic or digital signature, username, credit or debit card number, voice print, retina image, iris image, DNA profile, security related question or any other identification which are available for advance technology.	Verbatim, except two sentencing related changes. First, the maximum applicable prison sentence for the offence has been reduced by three years. Second, the higher mandatory imprisonment for repeat offenders has been removed.
27. Offence and punishment for committing cyber terrorism. (1) If any person (a) creates obstruction to make legal access, or makes or causes to make illegal access to any computer or computer network or internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or (b) creates pollution or inserts malware in any digital device which may cause or likely to cause death or serious injury to a person; or (c) affects or damages the supply and service of daily commodity of public or creates adverse effect on any critical information infrastructure; or (d) intentionally or knowingly gains access to, or makes interference with, any computer, computer network, internet network, any protected data-information or computer database, or gains access to any such protected data information or computer database which may be used against friendly relations with another foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group, then such person shall be deemed to have committed an offence of cyber terrorism. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both.	**27**. Offence and punishment for committing cyber terrorism. (1) If any person (a) creates obstruction to make legal access, or makes or causes to make illegal access to any computer or computer network or internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or (b) creates pollution or inserts malware in any digital device which may cause or likely to cause death or serious injury to a person; or (c) affects or damages the supply and service of daily commodity of public or creates adverse effect on any critical information infrastructure; or (d) intentionally or knowingly gains access to, or makes interference with, any computer, computer network, internet network, any protected data-information or computer database, or gains access to any such protected data information or computer database which may be used against friendly relations with another foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group, then the act of such person shall be cyber terrorism. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both.	Verbatim, except minor terminological changes in subsection 1(c) and removal of higher punishment applicable to repeat offenders.
28. Publication, broadcast, etc. of information in website or in any 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 electronic format which hurts religious	**28**. Publication, broadcast, etc. of information in website or in any 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 electronic format which hurts religious	Verbatim, except two sentencing related changes. First, the maximum applicable prison sentence for the offence has been reduced by three years and maximum applicable fine has been

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. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 20 (twenty) lac, or with both.	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. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 5 (five) lac, or with both.	reduced by five lac. Second, the higher mandatory imprisonment for repeat offenders has been removed.
29. Publication, transmission, etc. of defamatory information. (1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format, he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 5 (five) lac, or with both. (2) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 10 (ten) lac, or with both.	**29**. Publication, transmission, etc. of defamatory information. (1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format, then the act of such person shall be an offence, and for this, he shall be punished with fine not exceeding Taka 25 (twenty-five) lac.	Verbatim, except two sentencing related changes. First, prison sentence for the offence has been removed while maximum applicable fine has been increased by 20 lac. Second, the higher mandatory imprisonment for repeat offenders has been removed.
30. Offence and punishment for e-transaction without legal authority. (1) If any person (a) without legal authority, makes e-transaction over electronic and digital means from any bank, insurance or any other financial institution or any organisation providing mobile money service; or (b) makes any e-transaction though the e-transaction is, from time to time, declared illegal by the Government or Bangladesh Bank, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both. Explanation. For carrying out the purposes of this section, "e-transaction" means to deposit or withdraw money into or from any bank, financial institution or a specific account number through digital or electronic medium or to give direction or order for withdrawal, or legally authorized money transaction and transfer of money through any digital or electronic medium by a person for transferring his fund.	**30**. Offence and punishment for e-transaction without legal authority. (1) If any person - (a) without legal authority, makes e-transaction by digital or electronic means from any bank, insurance or any other financial institution or any organisation providing mobile money service; or (b) makes any e-transaction though the e-transaction is, from time to time, declared illegal by the Government or Bangladesh Bank, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with fine not exceeding Taka 25 (twenty-five) lac. Explanation. - For carrying out the purposes of this section, "e-transaction" means to deposit or withdraw money into or from any bank, financial institution or a specific account number through digital or electronic medium or to give direction or order for withdrawal, or legally authorized money transaction and transfer of money through any digital or electronic medium by a person for transferring his fund.	Verbatim, except two sentencing related changes. First, prison sentence for the offence has been removed while maximum applicable fine has been increased by 20 lac. Second, the higher mandatory imprisonment for repeat offenders has been removed.
31. Offence and punishment for deteriorating law and order, etc. (1) If any person intentionally publishes or transmits anything in website or digital layout that creates enmity, hatred or hostility among different classes or communities of the society, or destroys communal harmony, or creates unrest or disorder, or deteriorates or advances to deteriorate the law-and-order situation, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 5 (five) lac, or with both.	**31**. Offence and punishment for deteriorating law and order, etc. (1) If any person intentionally publishes or transmits anything in website or digital layout that creates enmity, hatred or hostility among different classes or communities of the society, or destroys communal harmony, or creates unrest or disorder, or deteriorates or advances to deteriorate the law-and-order situation, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both.	Verbatim, except two sentencing related changes. First, the maximum applicable prison sentence for the offence has been reduced by two years while maximum applicable fine has been increased by 20 lac. Second, the higher mandatory imprisonment for repeat offenders has been removed.

(3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 10 (ten) years, or with fine not exceeding Taka 10 (ten) lac, or with both.		
32. Offence and punishment for breaching secrecy of the Government. (1) If any person commits or abets to commit an offence under the Official Secrets Act, 1923 (Act No. XIX of 1923) by means of computer, digital device, computer network, digital network or any other digital means, he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both. (2) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 1 (one) crore, or with both.		Section 32 of the DSA was not retained in the final version of the CSA (although it was initially retained in the first draft of the CSA).
33. Punishment for holding, transferring data-information illegally, etc. (1) If any person preserves or abets to preserve any data-information of any governmental, semi-governmental, autonomous or statutory organisation, or any financial or commercial organisation by making illegal access to any of its computer or digital system in order to make any addition or deletion, or hand over or transfer, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka10 (ten) lac, or with both. (3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 15 (fifteen) lac, or with both.		Section 33 of the DSA was not retained in the CSA.
34. Offence related to hacking and punishment thereof. (1) If any person commits hacking, it shall be an offence, and for this, he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both. (2) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both. Explanation. In this section "hacking" means (a) to destroy, cancel or change any information of the computer data storage, or to reduce the value or efficacy of it or to cause harm in any way; or (b) to cause harm to any computer, server, computer network or any other electronic system by gaining access thereto without ownership or possession.	**32**. Offence related to hacking and punishment thereof. (1) If any person commits hacking, it shall be an offence, and for this, he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both. Explanation. - In this section "hacking" means - (a) to destroy, cancel or change any information of the computer data storage, or to reduce the value or efficacy of it or to cause harm in any way; or (b) to cause harm to any computer, server, computer network or any other electronic system by gaining access thereto without ownership or possession.	Verbatim, except removal of higher punishment applicable to repeat offenders.
35. Abetment of committing an offence and punishment thereof. (1) If any person abets to commit an offence under this Act, then such act of the person shall be an offence. (2) In case of abetment of committing an offence, the person abetted to commit the offence shall be punished with the same punishment as is provided for the offence.	**33**. Abetment of committing an offence and punishment thereof. (1) If any person abets to commit an offence under this Act, then such act of the person shall be an offence. (2) In case of abetment of committing an offence, the person abetted to commit the offence shall be punished with the same punishment as is provided for the offence.	Verbatim.
	34. Offence and punishment for filing false case, complaint, etc.-	An offence for filing false cases has been introduced

	(1) If any person, with intent of causing harm to another person, files or causes to file a case or a complaint against the person under any other section of this Act, knowing that there is no just or legal ground for filing a case or a complaint, then it shall be an offence and the person filing the case or the complaint and the person causing to file the case or the complaint shall be punished with the penalty prescribed for the original offence. (2) If any person files any case or a complaint under sub-section (1) under more than one section of this Act, the amount of penalty for the original offence for which the amount of penalty is the most among the offences mentioned in the said sections shall be determined as the penalty amount. (3) The Tribunal may, on the basis of a written complaint by any person, entertain and try cases of offences committed under sub-section (1).	anew in the Cyber Security Act 2023.
36. 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 exercised all due diligence to prevent the offence. (2) If the company referred to in sub-section (1) is a legal entity, it may be accused or convicted separately, in addition to accusing or convicting the persons mentioned above, but only fine may be imposed upon the company under the concerned provision. Explanation. In this section (a) "company" includes any commercial institution, partnership business, society, association or organization; (b) "director", in case of commercial institution, includes any partner or member of the Board of Directors.	**35**. 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 exercised all due diligence to prevent the offence. (2) If the company referred to in sub-section (1) is a legal entity, it may be accused or convicted separately, in addition to accusing or convicting the persons mentioned above, but only fine may be imposed upon the company under the concerned provision. Explanation. - In this section - (a) "company" includes any commercial institution, partnership business, society, association or organization; (b) "director", in case of commercial institution, includes any partner or member of the Board of Directors.	Verbatim.
37. Power to issue order for compensation. If any person causes financial loss to any other person by means of digital or electronic forgery under section 22, digital or electronic fraud under section 23 and identity fraud or personation under section 24, then the Tribunal may issue order to compensate the person affected with money equivalent to the loss caused, or such amount of money as it considers to be sufficient.	**36**. Power to issue order for compensation. If any person causes financial loss to any other person by means of digital or electronic forgery under section 22, digital or electronic fraud under section 23 and identity fraud or personation under section 24, then the Tribunal may issue order to compensate the person affected with money equivalent to the loss caused, or such amount of money as it considers to be sufficient.	Verbatim.
38. 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 breach was committed without his knowledge, or he exercised all due diligence to prevent the offence.	**37**. 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 breach was committed without his knowledge or exercised all due diligence to prevent the offence.	Verbatim.
39. Investigation, etc. (1) Any offence committed under this Act shall be investigated by a police officer, hereinafter in this chapter referred to as the Investigation Officer. (2) Notwithstanding anything contained in sub-section (1), if it appears at the beginning of the case or at any stage of investigation that to form an investigation team is necessary for fair investigation, then the Tribunal or the Government may, by order, form a joint investigation team comprising of the investigation agency, the law and order enforcement force and the agency under the control of such authority or agency and on such condition as may be referred to in the order.	**38**. Investigation, etc. (1) Any offence committed under this Act shall be investigated by a police officer, hereinafter in this chapter referred to as the Investigation Officer. (2) Notwithstanding anything contained in sub-section (1), if it appears at the beginning of the case or at any stage of investigation that to form an investigation team is necessary for fair investigation, then the Tribunal or the Government may, by order, form a joint investigation team comprising of the investigation agency, the law and order enforcement force and the agency under the control of such authority or agency and on such condition as may be referred to in the order.	Verbatim.

40. Time-limit for investigation, etc. (1) The Investigation Officer (a) shall complete the investigation within 60 (sixty) days from the date of getting charge of investigation of an offence; (b) may, if fails to complete the investigation within the time-limit prescribed under clause (a), extend the time-limit of investigation for further 15 (fifteen) days, subject to the approval of his controlling officer; (c) shall, if fails to complete the investigation within the time-limit prescribed under clause (b), inform the matter to the Tribunal in the form of a report with reasons to be recorded in writing, and shall complete the investigation within the next 30 (thirty) days with the permission of the Tribunal. (2) If any Investigation Officer fails to complete the investigation under sub- section (1), the Tribunal may extend the time-limit for the investigation up to a reasonable period.	**39**. Time-limit for investigation, etc. (1) The Investigation Officer (a) shall complete the investigation within 90 (ninety) days from the date of getting charge of investigation of an offence; (b) may, if fails to complete the investigation within the time-limit prescribed under clause (a), extend the time-limit of investigation for further 15 (fifteen) days, subject to the approval of his controlling officer; (c) shall, if fails to complete the investigation within the time-limit prescribed under clause (b), inform the matter to the Tribunal in the form of a report with reasons to be recorded in writing, and shall complete the investigation within the next 30 (thirty) days with the permission of the Tribunal.	Verbatim, except two changes. First, the maximum time-limit of investigation under subsection (1) has been increased by 30 (thirty) days. Second, section 40(2) of the Digital Security Act 2018, which allowed extension of time for investigation, has not been retained by the Cyber Security Act 2023.
41. Power of Investigation Officer. (1) In case of investigation of any offence under this Act, the Investigation Officer shall have the following powers, namely: (a) taking under his own custody any computer, computer programme, computer system, computer network or any digital device, digital system, digital network or any programme, data-information which has been saved in any computer or compact disc or removable drive or by any other means; (b) taking necessary initiatives to collect data-information of traffic- data from any person or agency; (c) taking such other step as may be necessary for carrying out the purposes of this Act. (2) For the interest of investigation of an offence, the Investigation Officer may take assistance from any specialist or any specialized organisation while conducting investigation under this Act	**40.** Power of Investigation Officer. (1) In case of investigation of any offence under this Act, the Investigation Officer shall have the following powers, namely: (a) taking under his own custody any computer, computer programme, computer system, computer network or any digital device, digital system, digital network or any programme, data-information which has been saved in any computer or compact disc or removable drive or by any other means; (b) taking necessary initiatives to collect data-information of traffic- data from any person or agency; (c) taking such other step as may be necessary for carrying out the purposes of this Act. (2) For the interest of investigation of an offence, the Investigation Officer may take assistance from any specialist or any specialized organisation while conducting investigation under this Act	Verbatim.
42. Search and seizure by warrant. If a police officer has reasons to believe that (a) any offence has been committed or is likely to be committed under this Act; or (b) any computer, computer system, computer network, data information related to an offence committed under this Act, or any evidence thereof has been preserved in any place or to a person, then he may, for reasons of such belief to be recorded in writing, obtain a search warrant upon an application to the Tribunal or the Chief Judicial Magistrate or the Chief Metropolitan Magistrate, as the case may be, and proceed with the following measures, namely: (i) taking possession of the data-information of traffic data under the possession of any service provider, (ii) creating obstruction, at any stage of communication, to any telegraph or electronic communication including recipient information and data-information of traffic data.	**41**. Search and seizure by warrant. - If a police officer has reasons to believe that (a) any offence has been committed or is likely to be committed under this Act; or (b) any computer, computer system, computer network, data-information related to an offence committed under this Act, or any evidence thereof has been preserved in any place or to a person, then he may, for reasons of such belief to be recorded in writing, obtain a search warrant upon an application to the Tribunal or the Chief Judicial Magistrate or the Chief Metropolitan Magistrate, as the case may be, and proceed with the following measures, namely: (i) taking possession of the data-information of traffic data under the possession of any service provider, (ii) creating obstruction, at any stage of communication, to any telegraph or electronic communication including recipient information and data-information of traffic data.	Verbatim.
43. Search, seizure and arrest without warrant. (1) If any police officer has reasons to believe that an offence under this Act has been or is being committed, or is likely to be committed in any place, or any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way, then he may, for reasons of such belief to be recorded in writing, proceed with the following measures, namely: (a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure; (b) to seize the computer, computer system, computer network, data information or other materials used in committing the offence or any document supportive to prove the offence; (c) to search the body of any person present in the place;	**42**. Search, seizure and arrest without warrant. (1) If any police officer has reasons to believe that an offence under this Act has been or is being committed, or is likely to be committed in any place, or any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way, then he may, for reasons of such belief to be recorded in writing, proceed with the following measures, namely: - (a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure; (b) to seize the computer, computer system, computer network, data- information or other materials used in committing the offence or any document supportive to prove the offence; (c) to search the body of any person present in the place;	Verbatim

(d) to arrest any person present in the place if the person is suspected to have committed or be committing an offence under this Act. (2) After concluding search under sub-section (1), the police officer shall submit a report on such search to the Tribunal.	(d) to arrest any person present in the place if the person is suspected to have committed or be committing an offence under this Act. (2) After concluding search under sub-section (1), the police officer shall submit a report on such search to the Tribunal.	
44. Preservation of information. (1) If the Director General, suo moto, or upon an application of the Investigation Officer, believes that it is necessary to preserve any data-information saved in a computer for the interest of an investigation under this Act, and there is possibility to damage, destroy or change the data information or to make unavailable, then he may require the person or institution in charge of the computer or computer system to preserve such data- information up-to 90 (ninety) days. (2) The Tribunal may, upon an application, extend the time-limit of preservation of such data-information for a period which may not exceed 180 (one hundred and eighty) days in aggregate.	**43**. Preservation of information. (1) If the Director General, suo moto, or upon an application of the Investigation Officer, believes that it is necessary to preserve any data-information saved in a computer or computer system for the interest of an investigation under this Act, and there is possibility to damage, destroy or change the data information or to make unavailable, then he may require the person or institution in charge of the computer or computer system to preserve such data-information up-to 90 (ninety) days. (2) The Tribunal may, upon an application, extend the time-limit of preservation of such data-information for a period which may not exceed 180 (one hundred and eighty) days in aggregate.	Verbatim, except addition of references to computer system in section 43(1).
45. Not to hamper the general usage of computer. (1) The Investigation Officer shall conduct investigation in such a way that the legal use of computer, computer system, computer network or any part thereof is not hampered. (2) Any computer, computer system or computer network or any part thereof may be seized, if (a) it is not possible to make access to the concerned computer, computer system, computer network or any part thereof; (b) there is possibility to damage, destroy or change the data- information or to be unavailable unless the concerned computer, computer system, computer network or any part thereof is seized to prevent an offence or stop an ongoing offence.	**44**. Not to hamper the general usage of computer. (1) The Investigation Officer shall conduct investigation in such a way that the legal use of computer, computer system, computer network or any part thereof is not hampered. (2) Any computer, computer system or computer network or any part thereof may be seized, if (a) it is not possible to make access to the concerned computer, computer system, computer network or any part thereof; (b) there is possibility to damage, destroy or change the data- information or to be unavailable unless the concerned computer, computer system, computer network or any part thereof is seized to prevent an offence or stop an ongoing offence.	Verbatim.
46 Assistance in investigation. The Investigation Officer may request any person or entity or service provider to provide information or assist in the investigation while conducting investigation of an offence under this Act, and if requested, the concerned person, entity or service provider shall be bound to provide information and necessary assistance to the Investigation Officer.	**45**. Assistance in investigation. The Investigation Officer may request any person or entity or service provider to provide information or assist in the investigation while conducting investigation of an offence under this Act, and if requested, the concerned person, entity or service provider shall be bound to provide information and necessary assistance to the Investigation Officer.	Verbatim.
47. Secrecy of the information obtained in course of investigation. (1) If any person, entity or any service provider provides or publishes any information for the interest of investigation, no suit or prosecution shall lie against the person, entity, or service provider. (2) All persons, entities or service providers related to the investigation under this Act shall maintain the secrecy of information related to the investigation. (3) If any person contravenes the provisions of sub-sections (1) and (2), then such contravention shall be an offence, and for such offence he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 1 (one) lac, or with both.	**46**. Secrecy of the information obtained in course of investigation. (1) If any person, entity or any service provider provides or publishes any information for the interest of investigation, no suit or prosecution shall lie against the person, entity, or service provider. (2) All persons, entities or service providers related to the investigation under this Act shall maintain the secrecy of information related to the investigation. (3) If any person contravenes the provisions of sub-sections (1) and (2), then such contravention shall be an offence, and for such offence he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 1 (one) lac, or with both.	Verbatim.
48. Cognizance of offence, etc. (1) Notwithstanding anything contained in the Code of Criminal Procedure, the Tribunal shall not take cognizance of any offence except upon a report made in writing by any police officer.	**47**. Cognizance of offence, etc. (1) Notwithstanding anything contained in the Code of Criminal Procedure, the Tribunal shall not take cognizance of any offence except upon a report made in writing by any police officer.	Verbatim.

(2) The Tribunal shall, while trying an offence under this Act, follow the procedure of trials before Courts of Session laid down in Chapter XXIII of the Code of Criminal Procedure subject to being consistent with the provisions of this Act.	(2) The Tribunal shall, while trying an offence under this Act, follow the procedure of trials before Courts of Session laid down in Chapter XXIII of the Code of Criminal Procedure subject to being consistent with the provisions of this Act.	
49. Trial of offence and appeal. (1) Notwithstanding anything contained in any other law for the time being in force, offences committed under this Act shall be tried by the Tribunal only. (2) Any person aggrieved with the judgment of the Tribunal may prefer an appeal before the Appellate Tribunal.	**48**. Trial of offence and appeal. (1) Notwithstanding anything contained in any other law for the time being in force, offences committed under this Act shall be tried by the Tribunal only. (2) Any person aggrieved with the judgment of the Tribunal may prefer an appeal before the Appellate Tribunal.	Verbatim.
50. Application of the Code of Criminal Procedure. (1) Save as anything contrary to the provisions of this Act, the provisions of the Code of Criminal Procedure shall be applicable to the investigation, trial, appeal and all incidental matters related to any offence under this Act. (2) The Tribunal shall be deemed to be a Court of Session, and may exercise all powers of a Court of Session while trying any offence under this Act or any other offence derived from it. (3) The person presenting the case in the Tribunal on behalf of the complainant shall be regarded as Public Prosecutor.	**49**. Application of the Code of Criminal Procedure. (1) Save as anything contrary to the provisions of this Act, the provisions of the Code of Criminal Procedure shall be applicable to the investigation, trial, appeal and all incidental matters related to any offence under this Act. (2) The Tribunal, the Appellate Tribunal and, as the case may be, the Police Officer in the while discharging the duties assigned to them, shall follow the provisions of Part-II and Part-III of Chapter VIII of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006) in accordance with the provisions of this Act, in respect of the following matters, namely: (a) Trial procedure of Tribunals and Appellate Tribunals, (b) Time limit to deliver judgment: (c) Penalties or forfeiture no bar against other punishments; (d) Power of detention or arrest in public place, etc.; (e) Procedure of search; and (f) Power of Appellate Tribunal and procedure for hearing and disposal of appeals.	Verbatim except two procedural changes: (i) procedure prescribed under Part-II and Part-III of Chapter VIII of the Information and Communication Technology Act, 2006 made applicable to cases under the Cyber Security Act 2023, under Section 50(2). (ii) Section 50(3) of the DSA has not been retained.
51. Taking opinion of experts, training, etc. (1) The Tribunal or the Appellate Tribunal may, during trial, take independent opinion from any person expert in computer science, cyber forensic, electronic communication, data security and in related other fields. (2) The Government or the Agency may, if necessary, provide specialized training to all persons concerned in the implementation of this Act, on computer science, cyber forensic, electronic communication, data security and other necessary matters.	**50**. Taking opinion of experts, training, etc. (1) The Tribunal or the Appellate Tribunal may, during trial, take independent opinion from any person expert in computer science, digital forensic, electronic communication, data security and in related other fields. (2) The Government or the Agency may, if necessary, provide specialized training to all persons concerned in the implementation of this Act, on computer science, digital forensic, electronic communication, data security and other necessary matters.	Verbatim.
52. Time-limit for disposal of case. (1) The judge of the Tribunal shall dispose of a case under this Act within 180 (one hundred and eighty) working days from the date on which the charge is framed. (2) If the judge of the Tribunal fails to dispose a case within the time-limit specified in sub-section (1), he may, for reasons to be recorded in writing, extend the time-limit up to 90 (ninety) days. (3) If the judge of Tribunal fails to dispose a case within the time-limit specified in sub-section (2), he may, with intimation to the High Court Division in the form of a report recording reasons thereof, continue the proceedings of the case.	**51**. Time-limit for disposal of case. (1) The judge of the Tribunal shall dispose of a case under this Act within 180 (one hundred and eighty) working days from the date on which the charge is framed. (2) If the judge of the Tribunal fails to dispose a case within the time-limit specified in sub-section (1), he may, for reasons to be recorded in writing, extend the time-limit up to 90 (ninety) days. (3) If the judge of Tribunal fails to dispose a case within the time-limit specified in sub-section (2), he may, with intimation to the High Court Division in the form of a report recording reasons thereof, continue the proceedings of the case.	Verbatim.
53. Offences to be cognizable and bailabe.In this Act (a) the offences specified in sections 17, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31, 32, 33 and 34 shall be cognizable and non-bailable; (b) the offences specified in clause (b) of sub-section (1) of section 18, sections 20, 25, 29 and sub-section (3) of section 47 shall be noncognizable and bailable; (c) the offences specified in clause (a) of sub-section (1) of section 18 shall be non-cognizable, bailable and subject to the permission of the court, be compoundable; and	**52**. Offences to be cognizable and bailabe. - In this Act - (a) the offences specified in sections 17, 19, 27 and 32 shall be cognizable and non-bailable; (b) the offences specified in clause (b) of sub-section (1) of section 18, sections 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32 and 46 shall be non- cognizable and bailable; (c) the offences specified in clause (a) of sub-section (1) of section 18 shall be non-cognizable, bailable and subject to the permission of the court, be compoundable; and	Verbatim except two procedural changes: (i) Offences under Sections 21, 22, 23, 24, 26, 28, 31 and 32 are no longer cognizable and non-bailable, but have been made non-cognizable and bailable instead. (ii) Section 53(d) which made repeat offences cognizable and non-bailable has been removed.

(d) the offences, if committed by a person for the second time or more, shall be cognizable and non-bailable.		
54. Forfeiture. (1) If an offence is committed under this Act, the computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument by means of which the offence has been committed shall be liable to forfeiture according to the order passed by the Tribunal. (2) Notwithstanding anything contained in sub-section (1), if the Tribunal is satisfied that the person, under whose control or possession the computer, computer system, floppy disk, compact disk or any other computer related material or instrument have been found, is not responsible for committing the offence related to the materials, then the said computer, computer system, floppy disk, compact disk, tape drive or any other related compute materials shall not be liable to forfeiture. (3) If any legal computer, computer system, floppy disk, compact disk, tape drive or any other related computer material is found with the computer, computer system, floppy disk, compact disk, tape drive or any other related computer material liable to forfeiture under sub-section (1), then those items shall also be liable to forfeiture. (4) Notwithstanding anything contained in other provisions of this section, if any computer belonging to any Governmental organisation or any statutory body or any material or instrument related thereto is used for committing an offence, it shall not be liable to forfeiture.	**53**. Forfeiture. (1) If an offence is committed under this Act, the computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument by means of which the offence has been committed shall be liable to forfeiture according to the order passed by the Tribunal. (2) Notwithstanding anything contained in sub-section (1), if the Tribunal is satisfied that the person, under whose control or possession the computer, computer system, floppy disk, compact disk or any other computer related material or instrument have been found, is not responsible for committing the offence related to the materials, then the said computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials shall not be liable to forfeiture. (3) If any legal computer, computer system, floppy disk, compact disk, tape drive or any other related computer material is found with the computer, computer system, floppy disk, compact disk, tape drive or any other related computer material liable to forfeiture under sub-section (1), then those items shall also be liable to forfeiture. (4) Notwithstanding anything contained in other provisions of this section, if any computer belonging to any Governmental organisation or any statutory body or any material or instrument related thereto is used for committing an offence, it shall not be liable to forfeiture.	Verbatim.
55. Regional and international cooperation. If any regional or international cooperation is necessary in case of investigating or trial of an offence committed under this Act, the provisions of the Mutual Assistance in Criminal Matters Act, 2012 (Act No. IV of 2012) shall be applicable.	**54**. Regional and international cooperation. If any regional or international cooperation is necessary in case of investigating or trial of an offence committed under this Act, the provisions of the Mutual Assistance in Criminal Matters Act, 2012 (Act No. IV of 2012) shall be applicable.	Verbatim.
56. Delegation of power. The Director General may, if necessary, by order in writing, delegate any of his powers or duties conferred upon him under this Act to any employee of the Agency and any other person or a police officer.	**55**. Delegation of power. The Director General may, if necessary, by order in writing, delegate any of his powers or duties conferred upon him under this Act to any employee of the Agency and any other person or a police officer.	Verbatim.
57. Actions taken in good faith. No suit or prosecution or any other legal proceeding shall lie against any employee or person concerned for any damage caused or likely to be caused to any person consequent to anything which is done in good faith under this Act.		Section 57 of the DSA was not retained in the CSA.
58. Evidentiary value. Notwithstanding anything contained contrary in the Evidence Act, 1872 (Act I of 1872) or any other law, any forensic evidence obtained or collected under this Act shall be admitted as evidence in the trial.	**56.** Evidentiary value. Notwithstanding anything contained contrary in the Evidence Act, 1872 (Act I of 1872) or any other law, any forensic evidence obtained or collected under this Act shall be admitted as evidence in the trial.	Verbatim
59. Removal of difficulty. If any difficulty arises in implementation of the provisions of this Act, the Government may, by notification in the official Gazette, take any necessary action in this behalf to remove such difficulty.	**57**. Removal of difficulty. If any difficulty arises in implementation of the provisions of this Act, the Government may, by notification in the official Gazette, take any necessary action in this behalf to remove such difficulty.	Verbatim
60. Power to make rules. (1) The Government may, by notification in the official Gazette, make rules for carrying out the purposes of this Act. (2) Without prejudice to the generality of sub-section (1), the Government may, inter alia, make rules especially for all or	**58**. Power to make rules. (1) The Government may, by notification in the official Gazette, make rules for carrying out the purposes of this Act. (2) Without prejudice to the generality of sub-section (1), the Government may, inter alia, make rules especially for all or	Verbatim

any of the following matters, by notification in the official Gazette, namely: (a) establishment of digital forensic lab; (b) supervision of digital forensic lab by the Director General; (c) review of traffic data or information and the process of its collection and preservation; (d) process of interference, review or decryption and protection; (e) security of critical information infrastructure; (f) procedure of regional and international cooperation in case of digital security; (g) formation and operation of Emergency Response Team and co- ordination with other teams; (h) cloud computing, metadata; and (I) protection of preserved data	any of the following matters, by notification in the official Gazette, namely: - (a) establishment of digital forensic lab; (b) supervision of digital forensic lab by the Director General; (c) review of traffic data or information and the process of its collection and preservation; (d) process of interference, review or decryption and protection; (e) security of critical information infrastructure; (f) procedure of regional and international cooperation in case of cybe security; (g) formation and operation of Emergency Response Team and co- ordination with other teams; (h) cloud computing, metadata; and (i) protection of preserved data.	
61. Amendment and savings of the Act No. XXXIX of 2006. (1) Upon the commencement of this Act, the sections 54, 55, 56, 57 and 66 of the Information and Communication Technology Act, 2006 (Act No. XXXIX of 2006), hereinafter referred to in this section as repealed sections, shall be repealed. (2) The proceedings or cases initiated before, or taken cognizance by, the Tribunal under the repealed sections specified in sub-section (1) shall, if pending at any stage of trial, continue as if the said sections had not been repealed.	**59**. Repeal and savings. (1) Digital Security Act, 2018 (Act No. XLVI of 2018), hereinafter referred to as the said Act, is hereby repealed. (2) Immediately prior to such repeal, pending cases under the said Act in the relevant Tribunal, and appeals against the order, judgment or sentence passed in similar cases in the relevant Appellate Tribunal, shall be conducted and disposed of as if the said Act had not been repealed. (3) All the cases in which a report or complaint has been made or a Charge Sheet has been submitted or the case is under investigation due to an offence under the said Act shall also be deemed to be a case under trial in the Tribunal referred to in sub-section (2). (4) Notwithstanding the repeal under sub-section (1), under the said Act— (a) all movable and immovable properties, documents and liabilities, if any, of the constituted Digital Security Agency shall be vested in the National Cyber Security Agency; (b) rules made orders, instructions, notifications or guidelines issued; or any measures made, notified or adopted shall, subject to their being consistent with the provisions of this Act, remain in force until repealed under this Act, and the same shall be deemed to have been made, notified or received under this Act; (c) all officers and employees including the Director General and Directors of the constituted Digital Security Agency shall be deemed to be the Director General, Directors and officers of the National Cyber Security Agency, and shall be deemed to be appointed and employed in the National Cyber Security Agency on the same terms as they were appointed or employed in the Digital Security Agency; (d) the National Computer Emergency Response Team and the Computer Emergency Response Team constituted shall be deemed to be the National Computer Emergency Response Team and the Computer Emergency Response Team constituted under this Act; (e) a digital forensic lab established shall be deemed to be a digital forensic lab established under this Act; (f) A computer system, network or information infrastructure declared as critical information infrastructure shall be deemed to be a declared critical information infrastructure under this Act.	Two procedural changes: (i) Addition of subsections (2) and (3) which allow pending cases filed under the Digital Security Act 2018 to be disposed under it (ii) Addition of subsection (4) which mainly facilitates the transition from the Digital Security Agency to the Cyber Security Agency.
62. Publication of English text. (1) After the commencement of this Act, the Government may, by notification in the official Gazette, publish an authentic English text of this Act. (2) In the event of conflict between the Bangla and the English text, the Bangla text shall prevail.	**60**. Publication of English text. (1) After the commencement of this Act, the Government may, by notification in the official Gazette, publish an authentic English text of this Act. (2) In the event of conflict between the Bangla and the English text, the Bangla text shall prevail.	Verbatim.

Annex 2: Changes made in the final version of the Cyber Security Act 2023 compared to the first draft published for public feedback

Section of the CSA (Unofficial Internal English Translation)	Analysis
2. Definitions. (1) In this Act, unless there is anything repugnant in the subject or context- (d) "Computer Emergency Response Team" or "Computer Incident Response Team" means the Computer Emergency Response Team or Computer Incident Response Team described in sub-section (2) of section 9; (u) "spirit of liberation war" means nationalism, socialism, democracy, and secularism which are the ideals which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle;	Minor terminological changes.
5. Establishment of Agency, Office, etc. (1) For carrying out the purposes of this Act, the Government shall, by notification in the official Gazette, establish an Agency to be called the National Cyber Security Agency consisting of 1 (one) Director General and such number of Directors as may be prescribed by the Rule. (2) The head office of the Agency shall be in Dhaka, but the Government may, if necessary, set up its branch offices at any place in the country outside of Dhaka. (3) The Agency shall be administratively attached to the Information and Communication Technology Division as a Department. (4) The powers, responsibilities, and functions of the Agency shall be prescribed by rules.	Minor terminological changes.
7. Manpower of the Agency. (1) The Agency shall have the necessary manpower according to the organizational framework approved by the Government. (2) The terms and conditions of employment of the manpower of the Agency shall be determined by Rules.	Minor terminological changes.
8. Power to remove or block some data-information. (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 Regulatory Commission, hereinafter referred to as BTRC, to remove or, as the case may be, block the said data-information. (2) If, subject to the analysis of data by the law and order enforcing force, there is reason to believe that any data- information published or propagated in digital media hampers the solidarity, financial activities, security, defence, religious values or public discipline 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. (3) If BTRC is requested under sub-sections (1) and (2), it shall, with intimation to the Government of the said matters, instantly remove or, as the case may be, block the data information. (4) For carrying out the purposes of this section, other necessary matters shall be prescribed by rules.	Minor terminological change to the wording of Subsection 8(2) which introduces the need for the Director General of the Cyber Security Agency to analyse data and have reasonable belief of harm before requesting it to be removed.
9. Computer Emergency Response Team. (1) For carrying out the purposes of this Act, there shall be a National Computer Emergency Response Team under the Agency, for discharging duties on full time basis. (2) Any critical information infrastructure declared under section 15 may, if necessary, form its own Computer Emergency Response Team or Computer Incident Response Team, with the prior approval of the Agency. (3) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall consist of the persons expert in cyber security and, if necessary, members of law and order enforcing force. (4) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge their duties in such manner as may be prescribed by rules, on full time basis.	Minor terminological change to title of the section.

(5) Without prejudice to the generality of sub-section (4), the National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge the following duties, namely: - (a) to ensure the emergency security of the critical information infrastructure; (b) to take immediate necessary measures for remedy if there is any cyber or digital attack and if the cyber or digital security is affected; or (c) to take necessary initiatives to prevent probable and imminent cyber or digital attack; (d) to take overall co-operational initiatives, including exchange of information with any similar type of foreign team or organization, for carrying out the purposes of this Act, with the prior approval of the Government; and (e) to do such other act as may be prescribed by rules. (6) The Agency shall supervise and make co-ordination among the National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Teams.	
12. National Cyber Security Council. (1) For carrying out the purposes of this Act, the National Cyber Security Council shall consist of the following members, namely: (a) Prime Minister,o Government of the People's Republic of Bangladesh, who shall be its Chairman; (b) Minister, State Minister or Deputy Minister of the Ministry of Post, Telecommunication and Information Technology; (c) Minister of the Ministry of Law, Justice and Parliamentary Affairs; (d) Advisor of ICT affairs to the Prime Minister (e) Principal Secretary to the Prime Minister; (f) Governor, Bangladesh Bank; (g) Secretary, Posts and Telecommunication Division; (h) Secretary, Information and Communication Technology Division; (i) Secretary, Public Security Division; (j) Foreign Secretary, Ministry of Foreign Affairs; (k) Inspector General of Police, Bangladesh Police; (l) Chairman, Bangladesh Telecommunication Regulatory Commission; (m) Director General, Directorate General of Forces Intelligence; (n) Director General, National Security Intelligence; (o) Director General, National Telecommunication Monitoring Centre; (p) Director General, National Cyber Security Agency (2) The Director General shall provide secretarial assistance to the Council to perform its functions (3) For carrying out the purposes of sub-section (1), the Council, in consultation with the Chairman, may, at any time, by notification in the official Gazette, co-opt any specialist as its member, on such terms and conditions as may be prescribed.	Minor terminological changes.
13. Power, etc. of the Council. (1) For implementation of the provisions of this Act and the rules made thereunder, the Council shall provide necessary direction and advice to the Agency. (2) The Council shall, inter alia, perform the following functions, namely: - (a) to provide necessary directions for remedy if cyber security is under threat; (b) to give advice for infrastructural development of cyber security and enhancement of its manpower and quality; (c) to formulate inter-institutional policies to ensure the cyber security; (d) to take necessary measures to ensure the proper application of this Act and rules made thereunder; and (e) to do such other act as may be prescribed by rules.	Minor change: subsection (3) removed.
18. Illegal access to computer, digital device, computer system, etc. and punishment. (1) If any person intentionally (a) makes or abets to make illegal access to any computer, computer system or computer network; or (b) makes or abets to make illegal access to any computer, digital device, computer system or computer network with intent to commit an offence, then such act of the person shall be an offence. (2) If any person (A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 6 (six) months, or with fine not exceeding Taka 2 (two) lac, or with both; (B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both. (3) If any offence under sub-section (1) is committed to a computer or computer system or computer network protected by critical information infrastructure, he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both.	Minor terminological change: reference to 'any computer, digital device, computer system or computer network' added in subsection 1(b).

21. Punishment for carrying out any hateful, confusing and defamatory campaign about liberation war, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag. (1) If any person, by means of digital or electronic medium, carries out or instigates to carry out any propaganda or campaign against the liberation war of Bangladesh, spirit of liberation war, father of the nation Bangabandhu Sheikh Mujibur Rahman, national anthem or national flag, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 1 (one) crore, or with both.	There are two minor terminological changes. First, the description of the offence now includes new broad terminologies such as 'hateful', 'confusing' and 'defamatory' and explicit reference to Bangabandhu Sheikh Mujibur Rahman as the father of the nation. Second, maximum applicable sentence for the offence has been reduced by two years.
24. Identity fraud or personation (1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network- (a) holds the identity of another person or exhibits the personal information of another person as his own in order to deceive or cheat; or (b) holds the personal identity of any person, alive or dead, as his own by forgery in order to- (i) get or cause to get benefit for himself or for any other person; (ii) acquire any property or any interest therein; (iii) cause harm to a natural person or individual, then such act of the person shall be an offence. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.	Minor terminological change.
27. Offence and punishment for committing cyber terrorism. (1) If any person (a) creates obstruction to make legal access, or makes or causes to make illegal access to any computer or computer network or internet network with an intention to jeopardize the integrity, security and sovereignty of the State and to create a sense of fear or panic in the public or a section of the public; or (b) creates pollution or inserts malware in any digital device which may cause or likely to cause death or serious injury to a person; or (c) affects or damages the supply and service of daily commodity of public or creates adverse effect on any critical information infrastructure; or (d) intentionally or knowingly gains access to, or makes interference with, any computer, computer network, internet network, any protected data-information or computer database, or gains access to any such protected data information or computer database which may be used against friendly relations with another foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group, then the act of such person shall be cyber terrorism. (2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both.	Minor terminological changes.
29. Publication, transmission, etc. of defamatory information. (1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format, then the act of such person shall be an offence, and for this, he shall be punished with fine not exceeding Taka 25 (twenty-five) lac.	Minor terminological change.
	Section 32 of the DSA was not retained in the final version of the CSA (although it was initially retained in the first draft of the CSA). This removal also alters the sequence of sections between the first draft of the CSA and the final version.
34. Offence and punishment for filing false case, complaint, etc.- (1) If any person, with intent of causing harm to another person, files or causes to file a case or a complaint against the person under any other section of this Act, knowing that there is no just or legal ground for filing a case or a complaint, then it shall be an offence and the person filing the case or the complaint and the person causing to file the case or the complaint shall be punished with the penalty prescribed for the original offence. (2) If any person files any case or a complaint under sub-section (1) under more than one section of this Act, the amount of penalty for the original offence for which the amount of penalty is the most among the offences mentioned in the said sections shall be determined as the penalty amount. (3) The Tribunal may, on the basis of a written complaint by any person, entertain and try cases of offences committed under sub-section (1).	An offence for filing false cases introduced.
52. Offences to be cognizable and bailabe. - In this Act - (a) the offences specified in sections 17, 19, 27 and 32 shall be cognizable and non-bailable; (b) the offences specified in clause (b) of sub-section (1) of section 18, sections 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, and 46 shall be non- cognizable and bailable; (c) the offences specified in clause (a) of sub-section (1) of section 18 shall be non-cognizable, bailable and subject to the permission of the court, be compoundable; and	Minor procedural change: offences under Sections 21 and 30 made non-cognizable and bailable offences.

59. Repeal and savings. (1) Digital Security Act, 2018 (Act No. XLVI of 2018), hereinafter referred to as the said Act, is hereby repealed. (2) Immediately prior to such repeal, pending cases under the said Act in the relevant Tribunal, and appeals against the order, judgment or sentence passed in similar cases in the relevant Appellate Tribunal, shall be conducted and disposed of as if the said Act had not been repealed. (3) All the cases in which a report or complaint has been made or a Charge Sheet has been submitted or the case is under investigation due to an offence under the said Act shall also be deemed to be a case under trial in the Tribunal referred to in sub-section (2). (4) Notwithstanding the repeal under sub-section (1), under the said Act— (a)all movable and immovable properties, documents and liabilities, if any, of the constituted Digital Security Agency shall be vested in the National Cyber Security Agency; (b) rules made orders, instructions, notifications or guidelines issued; or any measures made, notified or adopted shall, subject to their being consistent with the provisions of this Act, remain in force until repealed under this Act, and the same shall be deemed to have been made, notified or received under this Act; (c) all officers and employees including the Director General and Directors of the constituted Digital Security Agency shall be deemed to be the Director General, Directors and officers of the National Cyber Security Agency, and shall be deemed to be appointed and employed in the National Cyber Security Agency on the same terms as they were appointed or employed in the Digital Security Agency; (d) the National Computer Emergency Response Team and the Computer Emergency Response Team constituted shall be deemed to be the National Computer Emergency Response Team and the Computer Emergency Response Team constituted under this Act; (e) a digital forensic lab established shall be deemed to be a digital forensic lab established under this Act; (f) A computer system, network or information infrastructure declared as critical information infrastructure shall be deemed to be a declared critical information infrastructure under this Act.	Two minor procedural changes: (i) Subsections (2) and (3) added which allow pending cases filed under the Digital Security Act 2018 to be disposed under it. (ii) Subsection (4) added which mainly facilitates the transition from the Digital Security Agency to the Cyber Security Agency.

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US


info@amnesty.org


+44 (0)20 7413 5500

JOIN THE CONVERSATION


www.facebook.com/Amnesty


@Amnesty

REPACKAGING REPRESSION

THE CYBER SECURITY ACT AND THE CONTINUING LAWFARE AGAINST DISSENT IN BANGLADESH

After sustained pressure from civil society and the international community, Bangladesh finally repealed its draconian Digital Security Act (DSA) by enacting the Cyber Security Act (CSA) in its place. This briefing demonstrates how the CSA repackages almost all repressive features of the DSA and marks a continuation of the state's crackdown on civic space and human rights, particularly the right to freedom of expression in Bangladesh.

INDEX: ASA 13/8332/2024
AUGUST 2024
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL