



Reference: TG ASA 13/2023.4453

AI Index Number: ASA 13/7125/2023

22 August 2023

**Mohammad Yusuf**

Deputy Secretary (Legal Branch)  
Information and Communication Technology Division  
Government of the People's Republic of Bangladesh

by email: [mohammed.yousuf@ictd.gov.bd](mailto:mohammed.yousuf@ictd.gov.bd)

SUBJECT: FEEDBACK ON PROPOSED "CYBER SECURITY ACT" OF BANGLADESH

Dear Secretary Yusuf,

Amnesty International appreciates the Bangladeshi government's effort to seek feedback on the draft "Cyber Security Act, 2023", which, if enacted, would repeal the controversial Digital Security Act 2018 (DSA). When the new law was announced, the organization welcomed the Bangladeshi government's decision to repeal the DSA but cautioned that the new law must not replicate the same repressive features of the DSA.<sup>1</sup>

Our preliminary reading of the draft law leads us to conclude that the draft CSA retains the repressive provisions of the DSA which have persistently been used to threaten and restrict the right to freedom of expression in Bangladesh.

Our comparison of Chapter 6 of the CSA with that of the DSA shows that the draft law retains all but one of the offences contained in the DSA verbatim. The only changes the CSA makes are related to sentencing, which can be summarized as follows: lowering the maximum applicable prison sentence for eight offences, removing a sentence of imprisonment for two offences, increasing the maximum applicable fine for three offences and removing the higher applicable penalty for all repeat offences (see Annex I).

The right to freedom of expression is a fundamental human right guaranteed under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), to which Bangladesh is a state party. Article 19 of the ICCPR stipulates that "Everyone shall have the right to hold opinions without interference" and "Everyone shall have the right to freedom of expression." Similarly, Article 39 of Bangladesh's Constitution guarantees that "freedom of thought and conscience", 'the right of every citizen to freedom of speech and expression' and 'freedom of the press' are all encompassed within the fundamental right to freedom of thought and conscience, and of expression.

In its current form, the CSA, just like the DSA, and the Information and Communication Technology (ICT) Act that preceded it, can be used to intimidate, harass and arbitrarily arrest journalists, clampdown on peaceful dissent and silence critical opinions.<sup>2</sup> While there are certain other laws which also impermissibly restrict the right to freedom of expression (such as the Bangladesh Telecommunication Act 2001 and Pornography Control Act 2012),<sup>3</sup> the ICT Act and the DSA have been most frequently used to stifle peaceful dissent and undermine freedom of press. As of April 2018, 1,271 people are reported to have been charged under section 57 of the ICT Act while over 7,000 people were reported to have been charged under DSA as of January 2023.<sup>4</sup> The repressive section 57 of the ICT Act was replaced by draconian provisions of DSA, which are now set to be replaced by almost identical provisions in the draft CSA.

Both Article 19 of the ICCPR and Article 39 of the Constitution recognize that the right to freedom of expression is subject to permissible restrictions. However, as the two sections below will show the restrictions posed by CSA, like the restrictions posed 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. In line with Bangladesh's international human rights obligations and the recommendations of the Office of the High Commissioner for Human Rights (OHCHR) in its technical note on the DSA,<sup>5</sup> we believe that the CSA must not retain, as it currently does, provisions on overbroad offences from the DSA which may be used to restrict and undermine the right to freedom of expression, nor the overbroad powers of arrest and investigation given to the police.

### **Retention of provisions on five overbroad offences which may be used to restrict and undermine the right to freedom of expression**

The draft CSA retains **Sections 25, (publication of 'false or offensive information'), 29 (publication of 'defamatory information'), and 31 (punishment for 'deteriorating law and order')** of the DSA verbatim. The CSA leaves the substance of these offences unchanged, while only reducing the applicable penalties and removing provisions mandating higher penalties for repeat offenders (see Annex I). In 2021, Amnesty International had documented an alarming pattern whereby these three specific provisions of the DSA, i.e. Sections 25, 29 and 31, had been weaponized to target and harass dissenting voices, including those of journalists, activists, and human rights defenders (HRDs).<sup>6</sup> 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 criminalize "false, offensive, derogatory and defamatory information", in contravention of the ICCPR.<sup>7</sup> In retaining Sections 25, 29 and 31 of the DSA in the CSA, the potential to weaponize these provisions to silence peaceful dissent, as done under the DSA, remains unchanged.

Certain 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. Similarly, 'annoy', 'insult', 'humiliate' and 'spread confusion', are other vague and overly broad terms used in Section 25 which are also undefined. Due to the broadly worded nature of Section 25, it can and has acted as a catch-all provision to criminalize a wide range of conduct which consists of the legitimate exercise of the right to expression and opinion. Therefore, it should be removed.

While **Section 29** of the CSA makes defamation punishable by a sentence of fine, rather than imprisonment as under the DSA, defamation remains criminalized. The UN Human Rights Committee has advised States to avoid “penalizing or rendering unlawful untrue statements that have been published in error but without malice”.<sup>8</sup> 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’.<sup>9</sup>

**Section 31**, although termed “deteriorating law and order”, 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”. The lack of clear definitions has invited arbitrary applications of this provision under the DSA.<sup>10</sup> OHCHR has recommended that section 31 be amended to comply with article 20 of the ICCPR, so that speech is only criminalized within the narrow scope of incitement to hatred.<sup>11</sup>

CSA similarly retains **Sections 21** and **28** of the DSA verbatim which criminalize ‘making any kind of propaganda or campaign against liberation war, spirit of liberation war, father of the nation, national anthem or national flag’ and ‘publication, broadcast, etc. of information in website or in any electronic format that hurts the religious values or sentiment’ respectively. 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 penalize the expression of opinions about historical facts are incompatible with Article 19 of the ICCPR.<sup>12</sup> It has held that “The Covenant does not permit general prohibition of expressions of an erroneous opinion or an incorrect interpretation of past events”.<sup>13</sup> The OHCHR has recommended that Sections 21 and 28 be repealed.<sup>14</sup>

### **Retention of overbroad powers of arrest, investigation, and pretrial detention**

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 six sections of the DSA, including Section 21, remain cognizable and non-bailable under **Section 53** of the CSA. This means that the police can continue arresting individuals without obtaining a court warrant for these six offences under the CSA, and the possibility of bail in such cases will also be severely restricted.<sup>15</sup> This perpetuates the risk of pre-trial detention for individuals accused under these six sections.

**Section 42** of the CSA is identical to Section 43 of the DSA and continues to authorize 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. One of two overly permissive conditions needs to be fulfilled for the police to conduct such invasive search, seizure, or arrest. The police officers must believe: that a crime under the Act has occurred, is occurring or is likely to occur or that any evidence is likely to be lost, destroyed, deleted or altered or made unavailable in any way.<sup>16</sup> They are simply required to record the reasons for such belief.<sup>17</sup> The OCHR 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.<sup>18</sup>

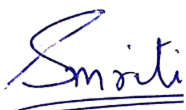
## Recommendations

In its current form, the CSA poses a grave threat to the rights to freedom of expression, privacy, and liberty in Bangladesh. The persistent use of the DSA and the ICT Act to target the media and journalists in the past decade provides a dangerous precedent that would allow to continue to clampdown on human rights unless the repressive features of the DSA are removed. In line with our concerns outlined above, Amnesty International urges Bangladesh's authorities to:

- Repeal the DSA and only enact another law in its place, such as the CSA, if and once it fully complies with international human rights law, including the ICCPR, to which Bangladesh is a state party.
- Remove sections 21, 25 and 28 of the CSA which criminalize legitimate expression of opinions or thoughts and have been used to stifle peaceful dissent under the DSA.
- Decriminalize 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.
- Remove overbroad, ambiguous, and vague terms from the CSA, such as Section 31, or provide sufficiently precise terminology that meets the test of legality, consistent with international human rights law.
- Amend provisions which allow overbroad powers of arrest, search, and seizure, such as 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.
- Amend section 53 of the CSA so that release pending trial is the general rule, while pre-trial detention is restricted to cases where a court finds specific, concrete, and compelling reasons to do so in the interest of justice or safety. Such a decision must be reviewed frequently and be subject to appeal.
- Hold public consultations, including with members of the press and civil society, in drafting any legislation and policy related to cyber space, such as the CSA, before they are approved by the cabinet or passed in parliament.
- Immediately and unconditionally release and drop all charges against all those accused under the DSA solely for peacefully exercising their right to freedom of expression.
- Introduce legislation to provide access to justice and effective remedies including adequate compensation for human rights violations, such as the rights to freedom of expression, privacy, and liberty.

We sincerely hope your government will take these recommendations into account.

Yours sincerely,



**Smriti Singh**

Interim Regional Director

South Asia Regional Office (SARO)

Amnesty International

## Annex I: Comparison of provisions of the CSA and DSA relating to offences and investigation powers

Provisions in DSA ( <a href="#">Official English Translation</a> )	Provisions in CSA (Unofficial English Translation)	Changes made (if any)
<p><b>17.</b> Punishment for illegal access to any critical information infrastructure.</p> <p>(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 tries 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</p> <p>(2) If any person</p> <p>(A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>7 (seven) years</b>, or with fine not exceeding Taka 25 (twenty-five) lac, or with both; and</p> <p>(B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>14 (fourteen) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p> <p>(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</p>	<p><b>17.</b> Punishment for illegal access to any critical information infrastructure.</p> <p>(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.</p> <p>(2) If any person -</p> <p>(A) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>3 (three) years</b>, or with fine not exceeding, or with both; and</p> <p>(B) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>6 (six) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Maximum applicable sentence for the offence under section 17(a) reduced by 4 (four) years.</p> <p>Maximum applicable sentence for the offence under section 17(b) reduced by 8 (eight) years.</p> <p>Higher punishment applicable for repeat offenders removed.</p>
<p><b>18.</b> Illegal access to computer, digital device, computer system, etc. and punishment.</p>	<p><b>18.</b> Illegal access to computer, digital device, computer system, etc. and punishment.</p>	<p>Verbatim</p> <p>Verbatim</p>

<p>(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.</p> <p>(2) If any person</p> <p>(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;</p> <p>(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.</p> <p>(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.</p> <p>(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.</p>	<p>(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 with intent to commit an offence, then such act of the person shall be an offence.</p> <p>(2) If any person</p> <p>(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;</p> <p>(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.</p> <p>(3) If any offence under sub-section (1) is committed to a computer or computer system or computer network <b>protected by critical information infrastructure</b>, 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.</p>	<p>Verbatim</p> <p>Reference to critical information infrastructure added</p> <p>Higher punishment applicable for repeat offenders removed</p>
---	---	--

<p><b>19. Damage of computer, computer system, etc. and punishment.</b></p>	<p><b>19. Damage of computer, computer system, etc. and punishment.</b></p>	<p>Verbatim</p>
<p>(1) If any person</p>	<p>(1) If any person</p>	
<p>(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</p>	<p>(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</p>	<p>Verbatim</p>
<p>(b) intentionally inserts or tries to insert any virus or malware or harmful software into any computer or computer system or computer network; or</p>	<p>(b) intentionally inserts or tries to insert any virus or malware or harmful software into any computer or computer system or computer network; or</p>	<p>Verbatim</p>
<p>(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</p>	<p>(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</p>	<p>Verbatim</p>
<p>(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</p>	<p>(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</p>	<p>Verbatim</p>
<p>(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</p>	<p>(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</p>	<p>Verbatim</p>
<p>(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,</p>	<p>(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,</p>	<p>Verbatim</p>

<p>of the person shall be an offence.</p> <p>(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.</p> <p>(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.</p>	<p>then such act of the person shall be an offence.</p> <p>(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.</p>	<p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed.</p>
<p><b>20.</b> Offence and punishment related to modification of computer source code.</p> <p>(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.</p> <p>(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.</p> <p>(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</p>	<p><b>20.</b> Offence and punishment related to modification of computer source code</p> <p>(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.</p> <p>(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.</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed.</p>



<p>exceeding 5 (five) years, or with fine not exceeding Taka 5 (five) lac, or with both.</p>		
<p><b>21.</b> 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.</p> <p>(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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>10 (ten) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p> <p>(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.</p>	<p><b>21.</b> 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.</p> <p>(1) If any person, by means of digital or <b>electronic</b> 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.</p> <p>(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 1 (one) crore, or with both.</p>	<p>Verbatim</p> <p>Reference to electronic medium added</p> <p>Maximum applicable sentence reduced by 3 three years.</p> <p>Higher punishment applicable for repeat offenders removed.</p>
<p><b>22.</b> Digital or electronic forgery</p> <p>(1) If any person commits forgery by using any digital or electronic medium, then such act of the person shall be an offence.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>5 (five) years</b>, or with</p>	<p><b>22.</b> Digital or electronic forgery</p> <p>(1) If any person commits forgery by using any digital or electronic medium, then such act of the person shall be an offence.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>2 (two) years</b>, or with</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Maximum applicable sentence reduced by 3 (three) years.</p>

<p>fine not exceeding Taka 5 (five) lac, or with both.</p> <p>(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.</p> <p>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.</p>	<p>fine not exceeding Taka 5 (five) lac, or with both.</p> <p>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.</p>	<p>Higher punishment applicable for repeat offenders removed.</p> <p>Verbatim</p>
<p><b>23. Digital or electronic fraud</b></p> <p>(1) If any person commits fraud by using any digital or electronic medium, then such act of the person shall be an offence.</p> <p>(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.</p> <p>(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.</p> <p>Explanation. - For carrying out the purposes of this section, “digital or electric fraud” means to change</p>	<p><b>23. Digital or electronic fraud</b></p> <p>(1) If any person commits fraud by using any digital or electronic medium, then such act of the person shall be an offence.</p> <p>(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.</p> <p>Explanation. - For carrying out the purposes of this section, “digital</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed.</p> <p>Verbatim</p>

<p>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.</p>	<p>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.</p>	
<p><b>24. Identity fraud or personation</b></p> <p>(1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network-</p> <p>(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-</p> <p>(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.</p> <p>(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.</p> <p>(3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished</p>	<p><b>24. Identity fraud or personation</b></p> <p>(1) If any person, intentionally or knowingly, by using any computer, computer programme, computer system, computer network, digital device, digital system or digital network-</p> <p>(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-</p> <p>(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.</p> <p>(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.</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed.</p>

<p>with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 10 (ten) lac, or with both.</p>		
<p><b>25.</b> Transmission, publication, etc. of offensive, false or threatening data- information</p> <p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>3 (three) years</b>, or with fine not exceeding Taka 3 (three) lac, or with both.</p> <p>(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.</p>	<p><b>25.</b> Transmission, publication, etc. of offensive, false or threatening data- information</p> <p>(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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>2 (two) years</b>, or with fine not exceeding Taka 3 (three) lac, or with both.</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Maximum applicable sentence reduced by 2 (two) years.</p> <p>Higher punishment applicable for repeat offenders removed.</p>
<p><b>26.</b> Punishment for unauthorized collection, use etc. of identity information.</p> <p>(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.</p>	<p><b>26.</b> Punishment for unauthorized collection, use etc. of identity information.</p> <p>(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.</p>	<p>Verbatim</p> <p>Verbatim</p>

<p>(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.</p> <p>(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.</p> <p>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.</p>	<p>(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.</p> <p>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.</p>	<p>Maximum applicable sentence reduced by 3 (three) years.</p> <p>Higher punishment applicable for repeat offenders removed.</p> <p>Verbatim</p>
<p><b>27. Offence and punishment for committing cyber terrorism.</b></p> <p>(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</p>	<p><b>27. Offence and punishment for committing cyber terrorism.</b></p> <p>(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</p>	<p>Verbatim</p> <p>Verbatim</p>

<p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>14 (fourteen) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p> <p>(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.</p>	<p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>14 (fourteen) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p>	<p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed</p>
<p><b>28.</b> Publication, broadcast, etc. of information in website or in any electronic format that hurts the religious values or sentiment.</p> <p>(1) If any person or group willingly or knowingly publishes or broadcasts or causes to publish or broadcast anything in website or</p>	<p><b>28.</b> Publication, broadcast, etc. of information in website or in any electronic format that hurts the religious values or sentiment.</p> <p>(1) If any person or group willingly or knowingly publishes or broadcasts or causes to publish or broadcast anything in website or</p>	<p>Verbatim</p> <p>Verbatim</p>

<p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>5 (five) years</b>, or with fine not exceeding Taka 10 (ten) lac, or with both.</p> <p>(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.</p>	<p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>2 (two) years</b>, or with fine not exceeding Taka 5 (five) lac, or with both.</p>	<p>Maximum applicable sentence reduced by 3 (three) years.</p> <p>Higher punishment applicable for repeat offenders removed</p>
<p><b>29.</b> Publication, transmission, etc. of defamatory information.</p> <p>(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 <b>3 (three) years</b>, or with fine not exceeding <b>Taka 5 (five) lac</b>, or with both.</p> <p>(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.</p>	<p><b>29.</b> Publication, transmission, etc. of defamatory information.</p> <p>(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 fine not exceeding <b>Taka 25 (twenty-five) lac</b>.</p>	<p>Verbatim</p> <p>Applicable prison sentence removed and maximum applicable fine increased by Taka 20 (twenty) lac.</p> <p>Higher punishment applicable for repeat offenders removed</p>
<p><b>30.</b> Offence and punishment for e-transaction without legal authority.</p> <p>(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</p>	<p><b>30.</b> Offence and punishment for e-transaction without legal authority.</p> <p>(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</p>	<p>Verbatim</p> <p>Verbatim</p>

<p>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.</p> <p>(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.</p> <p>(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.</p> <p>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.</p>	<p>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.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with fine not exceeding Taka 25 (twenty-five) lac.</p> <p>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.</p>	<p>Applicable prison sentence removed and maximum applicable fine increased by taka 20 (twenty) lac.</p> <p>Higher punishment applicable for repeat offenders removed</p> <p>Verbatim</p>
<p><b>31.</b> Offence and punishment for deteriorating law and order, etc.</p> <p>(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</p>	<p><b>31.</b> Offence and punishment for deteriorating law and order, etc.</p> <p>(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</p>	<p>Verbatim</p> <p>Verbatim</p>



<p>situation, then such act of the person shall be an offence.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>7 (seven) years</b>, or with fine not exceeding <b>Taka 5 (five) lac</b>, or with both.</p> <p>(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.</p>	<p>situation, then such act of the person shall be an offence.</p> <p>(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding <b>5 (five) years</b>, or with fine not exceeding <b>Taka 25 (twenty five) lac</b>, or with both.</p>	<p>Maximum applicable prison sentence reduced by 2 (two) years and maximum applicable fine increased by Taka 20 (twenty) lac.</p> <p>Higher punishment applicable for repeat offenders removed</p>
<p>32. Offence and punishment for breaching secrecy of the Government.</p> <p>(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 <b>14 (fourteen) years</b>, or with fine not exceeding Taka 25 (twenty five) lac, or with both.</p> <p>(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.</p>	<p><b>32.</b> Offence and punishment for breaching secrecy of the Government.</p> <p>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 or electronic means, he shall be punished with imprisonment for a term not exceeding <b>7 (seven) years</b>, or with fine not exceeding Taka 25 (twenty five) lac, or with both.</p>	<p>Verbatim</p> <p>Reference to electronic means added and maximum applicable prison sentence reduced by 7 (seven) years.</p> <p>Higher punishment applicable for repeat offenders removed</p>
<p>33. Punishment for holding, transferring data-information illegally, etc.</p> <p>(1) If any person preserves or abets to preserve any data-information of any governmental,</p>		<p>Section 33 of the DSA was not retained in the CSA.</p>

<p>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.</p> <p>(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.</p> <p>(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.</p>		
<p><b>34.</b> Offence related to hacking and punishment thereof.</p> <p>(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 <b>14 (fourteen) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p> <p>(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.</p> <p>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</p>	<p><b>33.</b> Offence related to hacking and punishment thereof.</p> <p>(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 <b>14 (fourteen) years</b>, or with fine not exceeding Taka 1 (one) crore, or with both.</p> <p>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</p>	<p>Verbatim</p> <p>Verbatim</p> <p>Higher punishment applicable for repeat offenders removed</p> <p>Verbatim</p>

<p>(b) to cause harm to any computer, server, computer network or any other electronic system by gaining access thereto without ownership or possession.</p>	<p>(b) to cause harm to any computer, server, computer network or any other electronic system by gaining access thereto without ownership or possession.</p>	
<p><b>35.</b> Abetment of committing an offence and punishment thereof.</p> <p>(1) If any person abets to commit an offence under this Act, then such act of the person shall be an offence.</p> <p>(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.</p>	<p><b>34.</b> Abetment of committing an offence and punishment thereof.</p> <p>(1) If any person abets to commit an offence under this Act, then such act of the person shall be an offence.</p> <p>(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.</p>	<p>Verbatim</p>
<p><b>36.</b> Offence committed by a company.</p> <p>(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.</p> <p>(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.</p> <p>Explanation. In this section (a) “company” includes any commercial institution, partnership business, society, association or organization;</p>	<p><b>35.</b> Offence committed by a company.</p> <p>(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.</p> <p>(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.</p> <p>Explanation. - In this section - (a) “company” includes any commercial institution, partnership business, society, association or organization;</p>	<p>Verbatim</p>

(b) "director", in case of commercial institution, includes any partner or member of the Board of Directors.	(b) "director", in case of commercial institution, includes any partner or member of the Board of Directors.	
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
<b>Chapter VII Investigation of Offences and Trial</b>		
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	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	Verbatim

<p>the agency under the control of such authority or agency and on such condition as may be referred to in the order.</p>	<p>the agency under the control of such authority or agency and on such condition as may be referred to in the order.</p>	
<p>40. Time-limit for investigation, etc.</p> <p>(1) The Investigation Officer (a) shall complete the investigation within <b>60 (sixty)</b> 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.</p> <p>(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.</p>	<p>39. Time-limit for investigation, etc.</p> <p>(1) The Investigation Officer (a) shall complete the investigation within <b>90 (ninety)</b> 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</p>	<p>Verbatim</p> <p>Maximum time-limit of investigation increased by 30 (thirty) days.</p> <p>Provision allowing extension of time-limit for the investigation removed.</p>

<p>41. Power of Investigation Officer.</p> <p>(1) In case of investigation of any offence under this Act, the Investigation Officer shall have the following powers, namely:</p> <p>(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;</p> <p>(b) taking necessary initiatives to collect data-information of traffic-data from any person or agency;</p> <p>(c) taking such other step as may be necessary for carrying out the purposes of this Act.</p> <p>(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</p>	<p>40. Power of Investigation Officer.</p> <p>(1) In case of investigation of any offence under this Act, the Investigation Officer shall have the following powers, namely:</p> <p>(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;</p> <p>(b) taking necessary initiatives to collect data-information of traffic-data from any person or agency;</p> <p>(c) taking such other step as may be necessary for carrying out the purposes of this Act.</p> <p>(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.</p>	<p>Verbatim</p>
<p>42. Search and seizure by warrant. If a police officer has reasons to believe that</p> <p>(a) any offence has been committed or is likely to be committed under this Act; or</p> <p>(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:</p> <p>(i) taking possession of the data-information of traffic data under</p>	<p>41. Search and seizure by warrant. - If a police officer has reasons to believe that -</p> <p>(a) any offence has been committed or is likely to be committed under this Act; or</p> <p>(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:</p> <p>(i) taking possession of the data-information of traffic data under</p>	<p>Verbatim</p>

<p>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.</p>	<p>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.</p>	
<p>43. Search, seizure and arrest without warrant.</p> <p>(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:</p> <p>(a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure;</p> <p>(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;</p> <p>(c) to search the body of any person present in the place;</p> <p>(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.</p> <p>(2) After concluding search under sub-section (1), the police officer shall submit a report on such search to the Tribunal.</p>	<p>42. Search, seizure and arrest without warrant.</p> <p>(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: -</p> <p>(a) to enter and search the place, and if obstructed, to take necessary measures in accordance with the Code of Criminal Procedure;</p> <p>(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;</p> <p>(c) to search the body of any person present in the place;</p> <p>(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.</p> <p>(2) After concluding search under sub-section (1), the police officer shall submit a report on such search to the Tribunal.</p>	<p>Verbatim</p>
<p>53. Offences to be cognizable and bailable. In this Act (a) the offences specified in sections 17, 19, 21, 22, 23, 24, 26,</p>	<p>52. Offences to be cognizable and bailable. - In this Act - (a) the offences specified in sections 17, 19, 21, 27, 30 and 33</p>	<p>Offences under Sections 22, 23, 24, 26, 28, 31 and 32 are no longer cognizable and non-bailable, but have been made</p>

<p>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 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 (d) the offences, if committed by a person for the second time or more, shall be cognizable and non-bailable.</p>	<p>shall be cognizable and non-bailable; (b) the offences specified in clause (b) of sub-section (1) of section 18, sections 20, 22, 23, 24, 25, 26, 28, 29, 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</p>	<p>non-cognizable and bailable instead</p>
--	---	--

## References

- <sup>1</sup> ‘Govt must ensure Cyber Security Act doesn’t rehash repressive features of DSA: Amnesty’, *Prothom Alo*, 07 August 2023, <https://en.prothomalo.com/bangladesh/lc37x1zp93> (Accessed 22 August 2023).
- <sup>2</sup> Amnesty International, *No Space for Dissent – Bangladesh’s Crackdown on Freedom of Expression Online* (2021), <http://www.amnesty.org/en/documents/asa13/4294/2021/en/>; Amnesty International, *Bangladesh: Muzzling dissent online* (2018), <https://www.amnesty.org/en/documents/asa13/9364/2018/en/>; Amnesty International, *Caught between fear and repression: Attacks on freedom of expression in Bangladesh* (2017), <https://www.amnesty.org/en/documents/asa13/6114/2017/en/> (Accessed 22 August 2023).
- <sup>3</sup> 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), [https://digitalcitizenbd.com/frontend/assets/documents/frdc\\_advocacy\\_brief.pdf](https://digitalcitizenbd.com/frontend/assets/documents/frdc_advocacy_brief.pdf) (Accessed 22 August 2023), p. 4.
- <sup>4</sup> ‘Law minister: Over 7,000 cases under DSA’, *Dhaka Tribune*, 05 June 2023 <https://www.dhakatribune.com/bangladesh/284852/law-minister-over-7-000-cases-under-dsa> (Accessed 22 August 2023).
- <sup>5</sup> Office of the United Nations High Commissioner for Human Rights, *OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act* (2022), <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf> (Accessed 22 August 2023).
- <sup>6</sup> Amnesty International, *No Space for Dissent – Bangladesh’s Crackdown on Freedom of Expression Online* (2021), <https://www.amnesty.org/en/documents/asa13/4294/2021/en/>, (Accessed 22 August 2023), pp. 16-17.
- <sup>7</sup> Ibid.
- <sup>8</sup> UN Human Rights Committee, General Comment No. 34, para 47.
- <sup>9</sup> Office of the United Nations High Commissioner for Human Rights, *OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act* (2022), <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf> (Accessed 22 August 2023).
- <sup>10</sup> Amnesty International, *No Space for Dissent – Bangladesh’s Crackdown on Freedom of Expression Online* (2021), <https://www.amnesty.org/en/documents/asa13/4294/2021/en/>; ‘Bangladesh: Teenage girl detained for Facebook post: Dipti Rani Das’, *Amnesty International*, 12 November 2018, <https://www.amnesty.org/en/documents/asa13/9364/2018/en/>;



---

'Bangladesh: Man faces 7 years in prison for Facebook post: Emdadul Haque Milon', *Amnesty International*, 11 March 2020, <https://www.amnesty.org/en/documents/asa13/1945/2020/en/> (Accessed 22 August 2023).

<sup>11</sup> Office of the United Nations High Commissioner for Human Rights, *OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act (2022)*, <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf> (Accessed 22 August 2023).

<sup>12</sup> UN Human Rights Committee, General Comment No. 34, para. 49.

<sup>13</sup> Ibid.

<sup>14</sup> Office of the United Nations High Commissioner for Human Rights, *OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act (2022)*, <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf> (Accessed 22 August 2023).

<sup>15</sup> Section 52 of the DSA cf Section 53 of the DSA.

<sup>16</sup> Section 42(1), CSA.

<sup>17</sup> Section 42(1), CSA.

<sup>18</sup> Office of the United Nations High Commissioner for Human Rights, *OHCHR Technical Note to the Government of Bangladesh on review of the Digital Security Act (2022)*, <https://www.ohchr.org/sites/default/files/documents/countries/bangladesh/OHCHR-Technical-Note-on-review-of-the-Digital-Security-Act-June-2022.pdf> (Accessed 22 August 2023).