রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, অক্টোবর ৬, ২০১৯

Government of the People's Republic of Bangladesh
Legislative and Parliamentary Affairs Division
Ministry of Law, Justice and Parliamentary Affairs

NOTIFICATION

Dated: 30 September, 2019 AD/15 Ashwin, 1426 BE

S.R.O. NO. 310-Law/2019.—In exercise of the powers conferred by section 62 of the Digital Security Act, 2018, the Government is pleased to publish the following English translation of the Act to be called the Authentic English Text of the Act, and it shall be deemed to have been effective from the date on which the Act comes into force under sub-section (2) of section 1 of the Act:

DIGITAL SECURITY ACT, 2018

Act No. XLVI of 2018

An Act to make provisions for ensuring digital security and identification, prevention, suppression and trial of offences committed through digital device and for matters ancillary thereto

WHEREAS it is expedient and necessary to make provisions for ensuring digital security and identification, prevention, suppression and trial of offences committed through digital device and for matters ancillary thereto;

THEREFORE, it is hereby enacted as follows:—

মূল্য : টাকা ২৪.০০

CHAPTER I
Preliminary

1. **Short title and commencement.—**(1) This Act may be called the Digital Security Act, 2018.

(2) It shall come into force at once.

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;

(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.

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.

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.

CHAPTER II
Digital Security Agency

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.

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.

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.

CHAPTER III
Preventive Measures

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.

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.

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.

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.

CHAPTER IV
Digital Security Council

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 Monitoring Centre (NTMC) or 1 (one) representative of mass media on recommendation of Ministry of Information].

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.

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.

CHAPTER V
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.

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.

CHAPTER VI
Offence and Punishment

17. **Punishment for illegal access to any critical information infrastructure, etc.**—(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 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.

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 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.

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,

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.

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.

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.

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 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.

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.

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.

(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.

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.

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 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.

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.

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.

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.

(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.

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.

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.

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.

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.

37. P**ower 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.

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.

CHAPTER VII
Investigation of Offence and Trial

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.

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.

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.

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.

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;

(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.

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.

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.

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.

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.

(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.

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.

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.

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.

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 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**.**

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 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.

CHAPTER VIII
Regional and International Cooperation

55. **Regional and international cooperation.—**If any regional or international cooperation is necessary in case of conducting an investigation or trial of an offence committed under this Act, the provisions of the the Mutual Assistance in Criminal Matters Act, 2012 (Act No. IV of 2012) shall be applicable.

CHAPTER IX
Miscellaneous

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.

57. A**ctions 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.

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 an evidence in the trial.

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.

60. P**ower 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 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.

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.

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.

By order of the President

মোঃ জাকির হোসেন
যুগ্মসচিব (লে. অ.)।

মোঃ তারিকুল ইসলাম খান, উপপরিচালক, বাংলাদেশ সরকারী মুদ্রণালয়, তেজগাঁও, ঢাকা কর্তৃক মুদ্রিত।
মোঃ আব্দুল মালেক, উপপরিচালক, বাংলাদেশ ফরম ও প্রকাশনা অফিস, তেজগাঁও,
ঢাকা কর্তৃক প্রকাশিত। website: www.bgpress.gov.bd