Registered No D A-1

Bangladesh Gazette

Additional Issue
Published by the Authority

Monday, October 8, 2018

Bangladesh Parliament

Dhaka, 23 Ashwin, 1426/08 October, 2018

The Parliament has accepted the following Act which has been approved by the President according to 23 Ashwin, 1425 on 08 October, 2018 and the Act is being published for information to public:--

Act No 46 of the Year 2018

The Act is enacted to ensure National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters

Whereas it is expedient and necessary to formulate an Act for ensuring National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters

It is, hereby enacted as follows: -

CHAPTER ONE

Preliminary

1) **Short Title and Commencement: -** (1) This Act shall be called Digital Security Act 2018
(2) It will come into force immediately

2) **Definition: -**
(1) Unless there is anything repugnant in the subject or context, in this Act,

a) "Appeal Tribunal" means the cyber appeal tribunal created under Section 82, information and communication technology Act, 2006 (Act No. 39 of year 2006);
b) "Data Storage" means text, image, information presented as audio or video format, knowledge, incident, principle idea or guidelines, which
   i) has been or is being formally produced by means of any computer or computer network or computer system; and
   ii) has been prepared with the aim of using it in any computer or computer network or computer system
c) " Agency" means Digital Security Agency formed 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 the communication process between one or more computer(s) or digital device(s) that are capable of collecting, sending and storing data singly or by connecting with each other;
f) "Council" means national digital security council formed under Section 12;
g) "Critical Information Infrastructure" means any physical or virtual information infrastructure declared by the government which is capable of controlling, processing, circulating or preserving any information, data or electronic information and which if it is damaged or compromised may adversely affect -
   (i) public safety or financial security or public health,
   (ii) national security or national integrity or sovereignty;
h) "Tribunal" means cyber tribunal created under Section 68 of, information and communication technology Act, 2006 (Act No. 39 of year 2006)**;**
i) "Digital" means the working procedure based on binary system (0 or 1) or digit based system, and to fulfill the objective of this Act, electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology will be the part of it;
j) " Digital Device" means any electronic, digital, magnetic, optical or information processing device or system which by using electronic, digital, magnetic, optical or information processing device or system, will perform logical, mathematical and memory programming, and any digital or computer device system or computer network connected with it or all kinds of input, output, processing, accumulating digital software device or communication facilities will be included;
k) "Digital Security" means the security of any digital device or digital system;
l) "Digital Forensic Lab" means the digital forensic lab formed under Section 10;
m) "Police Officer" means a police officer who is not below the rank of sub-inspector;
n) "Program" means any directives expressed in the form of sound, signal, writing or in any other form; produced with the help of a machine in a readable medium, using which any specific activity can be executed or be made tangibly productive using digital device
o) "Criminal Procedure" means Code of Criminal Procedure, 1898 (Act V of 1898);
p) "Person" means any person or institution, company, partnership business, farm or any other organization, in case of the digital device its controller, and any entity created by law or artificial legal entity will be included in it;
q) "Illegal Entrance" means entrance without the permission of any person or authority or entrance in violation of the conditions of permission of entrance by the said person or authority into any computer or digital device or digital network system, or by above mentioned entrance create hindrance in the exchange of any data-information suspend or prevent or stop the process of exchange of data-information, or change the data-information or add or deduct the data-information or collect the data-information with the use of a digital device

r) "Director General" means the director general of the agency;
s) "Defamation" means as defined under Section 499 of Penal Code (Act XLV of 1860)
t) "Malware" means such kind of computer or digital instruction, data-information, Program or application which-
    i) Is to change, distort, damage any work done by digital device or computer or to create adverse effect on the work done
    ii) Is to connect oneself to any computer or digital device and any Program of that mentioned computer or digital device, to operate data-information or during any other operation, it becomes autonomously active and by means of which the mentioned computer or digital device causes harmful incident or changes;
    iii) Is to create the opportunity of automatic entrance to a digital device or to steal information of the said device;
u) "Cognition of Liberation War" means those great ideals which inspired our brave public to dedicate themselves to the national liberation struggle and our brave martyrs to lay down their lives for the cause of liberation, the ideals of nationalism, socialism, democracy and secularism
v) "Service Provider" means:-
    i) Any person who through computer or digital process enables any user to communicate; or
    ii) Any such person, entity or institution who or which preserves or process data in favour of the service user

(2) The words and definition of expression used in this Act for which no definition has been provided in this Act it will ne deemed that those words and expression has been used in the meaning they are used in the, Information and communication technology Act, 2006.

3) Application of the act: -
If there is any conflict with the provision of this Act with any provision of any other Act,then the provisions of this Act will apply to the extent it is inconsistent with any other Act
However for any provisions relating to right to information the provisions of The Right to Information Act 2009 (Act no. 20 of 2009) will apply

4) Extra Judicial Application of the Act:-

1) If any person commits any offense within this Act outside Bangladesh which would be a punishable offense if committed inside Bangladesh, then the provisions of this Act would be applicable in such a manner as if those Acts were committed in Bangladesh
2) If any person commits any offense in Bangladesh within this Act from outside Bangladesh using any computer, computer system, or computer, then the provision of this Act will be applicable in such a manner as if the whole process of the offense was committed inside Bangladesh
3) If any person commits any offense outside Bangladesh within this Act from inside Bangladesh, then the provisions of this Act will be applicable in such a manner that the whole process of committing the offense occurred inside Bangladesh.

CHAPTER TWO

DIGITAL SECURITY AGENCY

5) Formation of agency, office, etc.:-

(1) To fulfill the objective of this Act, government, by notification in the official Gazette shall create an agency entitled as Digital Security agency consisting of 1 (one) Managing Director and 2 (two) Directors

(2) The headquarter of the agency will be in Dhaka, but if needed government, can establish branch office of the agency in any place in the country outside Dhaka.

(3) The responsibility, powers and functions of the Agency will be determined in accordance with rules.

6) Appointment of Managing Director, Directors, tenure etc.;-

(1) The government from the expert personnel in relation to the subject of computer or cyber security will appoint the Managing Director and the Directors and the terms of employment will be determined by the government.

(2) The Managing Director and the Directors will be the fulltime official of the agency, and they will follow the provisions of this Act and the Rules implemented under this Act in performing functions, exercising power, performing responsibilities as directed by the government

(3) If the position of the managing director is vacant, or if he/she is absent, sick or for any other reason is unable to fulfill his/her responsibility, then until a new managing director has been appointed in the vacant post, or until the Managing director has resumed his responsibilities, the senior most director will perform the responsibility of the Managing Director temporarily.

7) Agency Manpower: -

(1) The necessary manpower of the agency will be hired according to the organizational framework provided by the government.

(2) The agency can appoint necessary number of employees to properly perform its functions. The terms of employment will be determined by rules.

CHAPTER THREE

PREVENTIVE MEASURES

8) Power to remove or block some data-information:-

(1) If any data-information published or propagated in digital media regarding a subject that comes under the purview of Director General which threatens the Digital Security, then the Director General can request the Bangladesh Telecommunications and Regulatory Authority (BTRC) to remove or block the said Data-information as appropriate

(2) If it is evident to law and order enforcing security force that any data –information published or propagated in digital media hampers the nation or any part therein in terms of nations unity, financial activities, security, defense, religious values, public discipline or incites racism and hatred then the law and order enforcing Security force can request BTRC to block or remove the data-information via the Director General of the Agency.

(3) If the BTRC is requested as enshrined in subsection (1) and (2), BTRC will immediately notify the subject matter of the request to the government and remove or block the data-information as appropriate

(4) To fulfill the objective of the provision, other necessary subjects will be determined by rules

9) Emergency Response Team;-

(1) To fulfill the objective of this Act, there will be a national computer emergency response team under the agency, which will operate round the clock.
(2) Any Critical Information Infrastructure as defined in Section 15, can create its own computer emergency response team with prior permission from the agency
(3) Computer emergency response team will be formed by digital security expert personnel's and if necessary, will include members of law and order enforcing Security force.
(4) Computer emergency response team will operate round the clock performing their responsibilities as determined by rules.
(5) Without going against sub-section (4) as a whole, computer emergency response team will fulfill the responsibilities mentioned below, they are: -
    a. To ensure the security of Critical information infrastructure.
    b. If there is any cyber or digital attack or if the cyber or if cyber or digital security is hampered then take immediate necessary remedial measures
    c. To take necessary initiatives to prevent possible and upcoming cyber or digital attacks.
    d. To fulfill the objectives of this Act, with prior permission of the government, to take overall cooperation initiatives including information exchange with any similar type of international team or organization; and
    e. And other activities determined by rules.
(6) The agency will coordinate activities among Emergency response teams and also supervise them

10) Digital Forensic Lab: -

(1) To fulfill the objective of this Act, there will be one or more forensic lab under the control and supervision of the agency.
(2) No matter what is in Subsection (1), if a digital forensic lab was established under a government authority or institution before the enactment of this Act, the agency will give recognition to those forensic lab subject to the quality requirements under Section 11 of this Act and it will be deemed that those labs were established under this Act
(3) Agency will establish coordination between the digital forensic labs.
(4) The establishment of digital forensic lab, it uses, operations and other issues will be determined by rules.

11) Quality Control of Digital Forensic Lab:-

(1) The agency through quality standards determined by rules will ensure the quality of each Digital Forensic lab,
(2) In ensuring quality as per subsection (1), among other issues, each digital forensic lab-
    a. will have qualified and trained manpower to operate the activities of the lab;
    b. will ensure the physical infrastructural facilities;
    c. will take necessary measures to maintain the secrecy and security of the data-information
    d. to use instruments of quality in order to maintain the quality of the examination of digital technical standard; and
    e. All activities should be performed following scientific procedure and procedure determined by rules.

Chapter FOUR
Digital Security Council

12) National Digital Security Council:-

(1) To fulfill the objective of this Act, a National Digital Security Council will be formed consisting of 13 (thirteen) members including a chairman; as described below-
   a. Chairman
   b. Minister, State Minister or Deputy Minister of Ministry of Posts, Telecommunication and Information Technology;
   c. Minister, State Minister or Deputy Minister of Ministry of Law, Justice and Parliamentary Affairs
   d. Principal Secretary of the Prime Minister's Office;
   e. Governor, Bangladesh Bank;
   f. Secretary, Posts & 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, Defense Intelligence Head Office;
   m. Director General, National Digital Security Council; -Member Secretary

(2) The Prime Minister of Peoples Republic of Bangladesh will be the Chairman.

(3) To fulfill the objective of Subsection (1), with the advice/approval of the chairman, the council may co-opt as member at any time, a person with specialized knowledge or representative of a relevant body (for example: 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 a suitable representative from mass media on recommendation from Ministry of Information through gazette notification for a specified time and on specific terms.

13) The power of the Council, etc.: - (1) The Council in implementing the provisions of this Act and the Rules enacted under this Act will provide directives and advice to the agency

(2) The Council in addition to other subject matters will specially perform the following. Namely: -

   a. If the digital security is under threat provide necessary directions to remedy the situation;
   b. To advice on how to improve the digital security infrastructure; how to increase in its manpower and how to increase in its quality
   c. To enact inter-institutional policies with the aim of ensuring digital security:
   d. Taking necessary steps to ensure the implementation of the Act and of the Rules enacted under this Act; and
   e. Any other act determined by rules;

(3) Agency will provide necessary secretarial support to the council to perform its functions.

14) Council Meeting, Etc. (1) In lieu of provisions of this Section, council can decide its working procedures of the meeting.

(2) The meetings of the council will take place on a date, time and place as decided by its Chairman.

(3) Council will meet as and when necessary.

(4) The chairman will chair all council meetings.

(5) Any work or proceedings of the council will not be illegal because of the reason of a position being vacant or because of an error in the formation the council and no questions can be raised on it.

CHAPTER FIVE

Critical Information Infrastructure

15) Critical Information Infrastructure:- To fulfill the objective of this Act, government through government gazette may declare as critical information infrastructure any computer system, network or Information Infrastructure .

16) Visiting and Inspecting the security of Critical Information Infrastructure:-

(1) Director General, to ensure the conformance of the provisions of this Act will time to time visit and inspect the Critical information infrastructures and will submit a report to the government.

(2) The declared Critical information infrastructures within this Act, in a process determined by Rules will submit an investigative report regarding the internal and external infrastructure of it to the Government and notify The Director General about the subject matter of the report

(3) If the Director General reasonably believes that in a matter within his jurisdiction an act of any individual is threatening or harmful to any Critical Information Infrastructure he may by his own volition or by complaint of another start an investigation on the matter

(4) To fulfill the objective of this Act, expert personnel in the area of Digital Security shall complete the security visit or investigation activities on matters of Digital security.

CHAPTER SIX

Crime and Punishment

17) Punishment for Illegal Entrance in Critical Information Infrastructure, etc.: -

(1) If any person intentionally or knowingly in any Critical information infrastructure-

a. Illegally enters, or

b. By means of illegal entrance, harms or destroys or renders inactive the infrastructure or tries to do so,

Then the above activity of that person will be an offense under the Act

(2) If any person of Sub Section (1)-

a. Commits any offense within the Clause (a) then, the person will be penalized by imprisonment for a term not exceeding 7(seven) years or by fine not exceeding 25 (twenty five) lacs taka or with both.
b. Commits any offense within Clause (b) then, the person will be penalized by imprisonment for a term not exceeding 14 (fourteen) years or with fine not exceeding 1 (one) crore taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits the offense then, he will be punished with lifetime imprisonment or with fine not exceeding 5 (five) crore taka or with both

18) Illegal Entrance in computer, digital device, computer system, etc. and punishment:-

(1) If any person willingly-
a. illegally enters or help to enter in any computer, computer system or computer network, or
b. illegally enters or helps to enter with the intention of committing a crime then the activity of that person will be a offense under the Act

(2) If any person under Sub Section (1)-
a. Commits any offense within the Clause (a) then, the person will be penalized with imprisonment for a term not exceeding 6 months or by fine not exceeding3 (three) lacs taka or with both.
b. Commits any offense within Clause (b) then, the person will be penalized with imprisonment for a term not exceeding 3(three) years or with fine not exceeding 10 (ten) lacs taka or with both.

(3) If an offence within the Sub-Section (1), is committed in case of a secured computer or computer system or computer network then, the person will be penalized by imprisonment for a term not exceeding 3(three) years or by fine not exceeding 10 (ten) lacs taka or with both.

(4) If any person commits the offense within this Section for the second time or recurrently commits it then, he will be penalized with punishment that is two times of the punishment designated for the main offense

19) Damage of Computer, Computer System, etc. and punishment:-

(1) If any person-
a. Collects any data or data-storage, information or part of it from any computer, computer system, or computer network or collects transferable information or part of it or copy of it stored in the said computer, computer system or computer network, or
b. Intentionally inserts or tries to insert any virus or malware or any harmful software in any computer or computer system or computer network, or
c. Intentionally harms or tires to harm the data or data-storage of any computer, computer system, or computer network or harms or tries to harm the Programs protected in a computer, computer system, or computer network or
d. By any means stops or tries to stop a valid or authorized person to enter any computer, computer system, or computer network, or
e. Intentionally creates or tries to create spam or undesired emails without the permission of the sender or receiver, for any product or service marketing, or

f. Interferes unjustly in any computer, computer system or Computer network or by lies and deliberate falsity enjoys the service of an individual or transfers the charge or tries to transfer of such service into the account of another

Then, that person's activity will be a an offense under the Act

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 7(seven) years or fine not exceeding 10 (ten) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 10(ten) years of imprisonment or with fine not exceeding 25 (twenty five) lacs taka or with both.

20) Offenses relating to Computer Source Code Change and Punishment:-

(1) If any person intentionally or knowingly hides or destroys or changes the source code used in any computer, computer system, or computer network or if he tries to hide, destroy or change the source through another person and if that source code is preservable and securable then that act of the said person will be considered an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 3 (three) years or fine not exceeding 3 (three) lacs taka or with both

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 5(five) years or with fine not exceeding 5 (five) lacs taka or with both.

21) Punishment for Any propaganda or campaign against liberation war, Cognition of liberation war, Father of the nation, National Anthem or National Flag: -

(1) If any person by means of digital medium runs any propaganda or campaign or assists in running a propaganda or campaign against the liberation war of Bangladesh, Cognition of liberation war, Father of the Nation, National Anthem or national Flag then, that act of that person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 10 (ten) years or with fine not exceeding 1 (one) crore taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with life term imprisonment or with fine not exceeding 3 (three) crores or with both

22) Digital or Electronic Forgery:-

(1) If any person commits forgery by means of any digital or electronic medium then that activity of that particular person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 5 (five) lacs taka or with both

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both

Explanation:-

To fulfill the objective of this Act, **"Digital or Electronic Forgery"** means, if any person without authority or in excess of the given authority or by means of unauthorized practice produces input or output of any computer or digital device or changes, erases or hides incorrect data or program, or results in erroneous information, or information system of any computer or digital device, data system and computer or digital network operation

23) Digital or Electronic Fraud:-

(1) If any person commits fraud by means of any digital or electronic medium then that activity of that particular person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or by fine not exceeding 5 (five) lacs taka or with both

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both

Explanation:-
To fulfill the objective of this Act**, "Digital or Electric Fraud"** means, if any person intentionally or knowingly or without permission changes any information, deletes, adds new information or creates distortion and reduces the value of that or the utility of any computer program, computer system, computer network, digital device, digital system, digital network, or of a social communication medium, trying to gain benefit for himself/herself or for others or trying to harm others or to deceive others .

24) Identity Fraud or Being in Disguise:-

(1) If any person intentionally or knowingly uses any computer, computer Program, computer system, computer network, digital device, digital system or digital network-
   a. With the intention of deceiving or cheating carries the identity of another person or shows any person's identity as his own, or
   b. Intentionally by forgery assuming the identity of a alive or dead person as one's own for the following purpose-

      i. To achieve some advantages for oneself or for any other person;

ii. To acquire any property or interest in any property;
iii. To harm a person by using another person's identity in disguise.

Then the Act of the person will be an offense under the Act

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized by imprisonment for a term not exceeding 5 (five) years or fine not exceeding 5 (five) lacs taka or both

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 7 (seven) years or with 10 (ten) lacs taka or with both

25) Publishing, sending of offensive, false or fear inducing data-information, etc.:-

(1) If any person in any website or through any digital medium-
   a. Intentionally or knowingly sends such information which is offensive or fear inducing, or which despite knowing it as false is sent, published or propagated with the intention to annoy, insult, humiliate or denigrate a person or
   b. Publishes or propagates or assists in publishing or propagating any information with the intention of tarnishing the image of the nation or spread confusion or despite knowing it as false, publishes or propagates or assists in publishing or propagates information in its full or in a distorted form for the same intentions
   ,
   Then, the activity of that person will be an offense under the Act.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 3(three) years of or fine not exceeding 3(three) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with imprisonment for a term not exceeding 5(five) years or with fine not exceeding 10 (ten) lacs taka or with both

26) Punishment for Collecting, Using sIdentity Information without Permission, etc :-

(1) If any person without any legal authority collects, sells, takes possession, supplies or uses any person's identity information, then, that activity of that person will be an offense under the Act.
(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 5 (five) years or fine not exceeding 5 (five) lacs taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be penalized with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 10 (ten) lacs taka or with both.

Explanation:-

To fulfill the objective 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, his/her name, address, Date of birth, mother's name , father's name, signature, National identity , birth and death registration number, finger print, passport number , bank account number , driver's license , E-TIN number, Electronic or digital signature , username, Credit or debit card number, voice print , retina image , iris image , DNA profile, Security related questions or any other identification which due to the excellence of technology is easily available.

27) Punishment for committing Cyber-terrorism: -

(1) If any person –

a. With the intention to breach the national security or to endanger the sovereignty of the Nation and to instill terror within the public or a part of them creates obstruction in the authorized access to any computer, computer network or internet network or illegally accesses the said computer, computer network or internet network or cause the act of obstruction of access or illegal entry through someone, or

b. Creates such pollution within any digital device or inserts malware which causes in the death of a person or results in serious injury to a person or raises a possibility of it, or

c. Damages or destroys the supply of daily necessities of public or adversely affects any critical information infrastructure

d. Intentionally or knowingly enters or penetrates any computer, computer network, internet network, any secured data information or computer database or such secured data information or computer database which can be used to damage friendly relations with another foreign country or can be used for acts against public order or which can be used for the benefit any foreign country or any foreign person or any group.

Then that activity of that person will be considered as cyber security crime.

(2) If any person commits any offense mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding 14(fourteen) years or with fine not exceeding 1(one) crore taka or with both.

(3) If any person commits the offense mentioned in sub-section (1) for the second time or recurrently commits it then, he will be punished with lifetime imprisonment or with fine not exceeding 5(five) crore taka or with both

28) Publication, Broadcast, etc. of such information in any website or in any electronic format that hampers the religious sentiment or values:-

(1) If any person or group intentionally or knowingly with the aim of hurting religious sentiments or values or with the intention to provoke publish or broadcast anything by means of any website or any electronic format which hurts religious sentiment or values then such activity of that person will be considered an offence

(2) If any person commits an offence under sub section (1), the person will be sentenced to a term of imprisonment not exceeding 7 (seven) years or fine not exceeding 10 (ten) lac or both.

(3) If any person commits the offence mentioned in sub-section (1) second time or repeatedly, he will be punished with imprisonment not exceeding 10 (ten) years or fine not exceeding 20 (twenty) lac taka or both

29) To publish, broadcast, etc., defamation information:-

(1) If a person commits an offence of publication or broadcast defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in any website or in any other electronic format then he will be sentenced to a term of imprisonment not exceeding 3(Three) years or fine not exceeding Tk.5 (Five) lac or both.

(2) If any person commits the offence mentioned in sub-section (1) second time or repeatedly, he he will be sentenced to a term of imprisonment not exceeding 5(Five) years or fine not exceeding Tk.10 (Ten) lac or both

30) E-Transaction without legal authority Offence and Punishment:-

(1) If any person-

a. Does e-transaction through electronic and digital medium of any bank, insurance, or any other financial institution or any mobile money service providing organisation without legal authority, or.
b. Does e-transaction that has been declared illegal by the Government or Bangladesh Bank,.

Then such activity will be considered as an offence.

(2) If any person commits offence mentioned in sub section (1), the person will be penalized with either maximum of 5(five) years of imprisonment or fine of Tk. 5 (five) lac or will be punished with both.

(3) If any person commits the offence mentioned in sub-section (1) for the second time or repeatedly, he will be punished with a maximum of 7(seven) years imprisonment or with maximum fine of Tk. 10 (ten) lac or both.

Explanation:-

To fulfill the objective of this Section, **"E-Transaction", means deposit or withdrawal of fund or direction, order or legally authorized money transaction for withdrawal** through any bank, financial institution or through any digital or electronic medium to a specified account number by a person with the aim of transferring funds..

31) Deterioration of Act-order, etc. and Punishment:-

(1) If any person intentionally publish or broadcast any kind of file in any website or digital format which will create hostility, hatred or adversity among people or destroy any communal harmony or create unrest or disorder or deteriorates or threatens to deteriorate the law and order then that activity of that person will be considered as an offence..

(2) If any person commits any crime mentioned within sub section (1), the person will be penalized with imprisonment for a term not exceeding to 7(seven) years or fine not exceeding Tk. 5(five) lac or with both.

(3) If any person commits the crime mentioned in sub-section (1) for the second time or recurrently commits it, he will be punished with imprisonment for a term not exceeding 10(ten) years or with fine not exceeding Tk.10 (ten) lac or with both

32) Breaching Government Secret Offence and Punishment:-

(1) If any person commits or aids and abets in committing an offence under Official Secrets Act, 1923 (Act No XIX of 1923) through computer, digital device, computer network, digital network or through any other digital medium then he will be punished to a term of imprisonment not exceeding 14(fourteen) years or with fine not exceeding Tk.25 (Twenty Five) Lac or with both.

(2) If any person commits the offence mentioned in sub-section (1) for the second time or recurrently commits it, he will be punished with life imprisonment or with fine not exceeding Tk. 1(one) crore or with both.

33) Illegal Transferring, Saving etc. of Data-Information, Punishment:-

(1) If any person enters any computer or digital system illegally and does any addition or subtraction, transfer or with the aim of transfer save or aid in saving any data-information belonging to government, semi-government, autonomous or statutory organization or any financial or commercial organisation , then the activity of that person will be considered an offence.

(2) If any person commits an offence mentioned in sub section (1), he will be sentenced to a term of imprisonment not exceeding 5(Five) years or with fine not exceeding Tk.10 (Ten) lac or with both.

(3) If any person commits the offence mentioned in sub-section (1) second time or recurrently commits it then, he will be sentenced to a term of imprisonment not exceeding 7(Seven) years or with fine not exceeding Tk.15 (Fifteen) lac or with both.

34) Hacking Related Offence and Punishment:-

(1) If a person commits hacking then it will be considered an offence. and for this, he will be sentenced to a term of imprisonment not exceeding 14(Fourteen) years or with fine not exceeding Tk.1 (One) Crore or with both.

(2) If any person commits the offence mentioned in sub-section (1) second time or repeatedly then, he will be penalized with life imprisonment or with fine not exceeding Tk.5 (Five) Crore or both

Explanation:
In this section "Hacking" means-

a. To destroy, change, format, cancel any information of the compute data storage or to reduce the value or suitability of it or damaging it in any other way, or
b. Without ownership or possession illegally entering and damaging any computer, server, computer network, or any electric system

35) Aiding in Commission of Offence and its Punishment:-

(1) If any person aids in committing any offence under this Act then such act of that person will be considered an offence.

(2) In case of aiding of an offence, the punishment will be the same as that of the original offence.

36) Offence Committed by Company:-

(1) In case of a company committing an offence under this Act, all such owner, chief executive, director, manager, secretary, shareholder or any other officer or employee or representative of the company having direct connection with the offence will be considered as the offender unless he can prove that the offence took place without his knowledge or he took all possible steps to stop the commission of the offence

(2) If the company mentioned under subsection (1) is a company having corporate legal personality, then apart from the people mentioned, the company can also be charged and found guilty under the same proceedings, but only the monetary punishment can be imposed on the company as per the relevant provisions

Explanation:
In this Section-

a. The word "Company" includes any commercial institution, business partnership, society, association or organization;
b. In case of commercial organization meaning of "Director "will be regarded as including its shareholder or member of board of directors.

37) The power to give order of compensation:

If a person cause financial damage to another person under Section 22 digital or electronic forgery, under Section 23 digital or electric fraud and under Section 24 identification fraud or by means of disguise, the tribunal, may order him to compensate the affected person by giving money equivalent to the damage caused or a suitable amount after considering the damage caused

38) No Responsibility for the service provider:

(1) Any service provider will not be responsible under this Act or any rules enacted under this Act for facilitating access to data-information, if he succeeds in proving that, the offence or breach was committed without his knowledge or he took all possible steps to stop the commission of the offence. .

CHAPTER SEVEN

INVESTIGATION OF OFFENCE AND TRIAL

39) Investigation, etc.-

(1) Police Officer, hereinafter mentioned as the investigation officer in this chapter, will investigate offence committed under this Act.

(2) Irrespective of the provision in Sub Section (1), if, before starting trial or at any stage of investigation it is evident that, an investigation team is required for fair investigation of the case in question then by order of the tribunal or the government, under the control and conditions of the authority or organization mentioned in that order, investigation organization, with combination of Law and Security Enforcement Authority and Agency. can form a Joint Investigation team.

40) Time limit of Investigation, etc.: -

(1) Investigation officer-

a. Shall complete the investigation within 60 days from the date of getting charge of the investigation

b. If he fails to finish the investigation within the time mentioned in sub-section (a) then with the permission of his controlling officer, he can extend the time limit for investigation to another 15(fifteen) days

c. If he fails to finish the investigation within the time mentioned in sub-section (b), then he will record the reason and bring the matter to the knowledge of Tribunal in the form of a report,. and with the permission of the tribunal, he will complete the investigation within the next 30 (thirty) days.

(2) If any investigating officer fails to finish the investigation under Sub Section (1), then the tribunal may extend the time limit of the investigation up to a reasonable period.

41) Power of Investigation Officer: -

(1) While investigating any offence under this Act, the investigation officer shall have the following powers, such as:-

a. He/she can take in his/her custody computer, computer Program, computer system, computer network or any digital device, digital system, digital network or any Program, data-information which has been saved in any computer or compact disc or removable drive or in any other way;.

b. He/she can take necessary initiative to collect data-information from traffic-data from any person or organization.

c. Any other task necessary to fulfill the objectives of this Act.

(2) While conducting investigation under this Act the investigation officer may take help from any expert person or any specialized organization for the sake of investigation of an offence.

42) Search and Seizure through Warrant: -

If any police office has reason to believe that,

a. or An offence has been committed or there is possibility of commission of an offence under this Act, or-

b. Any computer, computer system, computer network, data-information relating to an offence under this Act, or any evidence-proof thereof is being kept in some place or with a person,

Then, he/she can after recording the reason for such belief, apply to the tribunal or as the case may be, to the Chief Judicial Magistrate or Chief Metropolitan Magistrate to obtain search warrant and do the below mentioned tasks :

i. To seize any traffic data which is under possession of any service provider,

ii. At any level of communication create obstruction to any telegraph or electronic communication containing recipient information and any data traffic including data-information

43) Search, Seizure and Arrest without Warrant: -

(1) If a police officer has a reason to believe that an offence under this Act has been or is being or will be committed in any place, or there is a possibility of it happening, or if there is a possibility of evidence being lost, destroyed, deleted or altered or possibility of it being made scarce in some other way, then the officer, upon recording the reason for his/her belief, can undertake the following tasks: -

a. Enter and search the said place and, if interrupted, take necessary action in accordance with the Code of Criminal Procedure;.

b. Seize the computer, computer systems, computer network, data-information or other objects which were used in committing the offence or documents that can aid in proving the offence that are found in that place while conducting the search;;

c. Conduct physical search of any person present in that place;

d. Arrest anyone present in the said place if suspected of committing or having committed an offence under this Act.

(2)) After conducting a search under subsection (1), the police officer will submit a search report to the Tribunal.

44) Data Preservation:-

(1) If the Director General on his own accord or on the basis of an application by the investigation officer believes that, any data-information stored in a computer should be preserved for the interest of an investigation under this Act or there is possibility that such information could be harmed, destroyed, altered or lost e, then, he/she can order the person or institution responsible for that computer or computer system to preserve such data-information for 90(ninety) days.

(2) Tribunal may, on application, extend the period of preservation of such data-information but it should not be for more than a total of 180 (one hundred and eighty) days.

45) Not to Interrupt the general usage of computer: -

(1) The investigation officer should run the investigation in such a way that,

the legal use of computer, computer system, computer network or any part thereof; is not interrupted.

(2) Any computer, computer system or computer network or parts of can be seized if

a. It is not possible to enter the concerned computer, computer system, computer network or any part of it
b. If the concerned computer, computer system, computer network or any part of it is not seized to stop commission of an offence or stop an ongoing offence, there is possibility of the data- information being harmed, destroyed, altered or lost.

46) Help In Investigation:-

The Investigation Officer while conducting investigation of an offence under this Act may request any person or entity or service provider to provide information or for providing assistance in the investigation and on such request the person, entity or service provider will be bound to help the Investigation Officer.

47) Secrecy of the Information obtained in the Investigation:-

(1) if any person, entity or any service provider gives or publishes any information for the interest of investigation then no proceedings can be brought against that person, entity, or service provider under civil or criminal law.
(2) All person, entity or service provider related with the investigation under this Act shall maintain secrecy of information related to the investigation.
(3) If any person breaches the provisions of Sub sections (1) and (2), then the breach will be considered as an offence, and for such offence he will be sentenced to a term of imprisonment not exceeding 2(Two) years or fine not exceeding Tk.1 (One) lac or both

48) Cognizance of Offence, etc. :-

(1) irrespective of the provisions of the Code of Criminal Procedure, , the Tribunal will not take cognizance of an offence without written report of police officer.
(2) Tribunal will follow the procedures for trial of Sessions Court as mentioned in Chapter 23 of the Code of Criminal Procedure, so far as they are compatible with the provisions of this Act while conducting trial of offence under this Act.

49) Adjudication of Offence and Appeal:-

(1) Notwithstanding provisions of any other law that are currently in force, offence committed under this Act will be tried by the Tribunal exclusively.
(2) Any person aggrieved by the judgment of the tribunal may appeal in the Appeal Tribunal.

50) Application of forgery code of conduct: -

(1) Provided there is nothing contrary in the Act, the investigation of the offence, adjudication, appeal and settlement of other issues, the provisions of Code of Criminal Procedure will be applicable..
(2) The Tribunal will be regarded as a Session Court and while adjudicating any offence under this Act or any offence related to it , the tribunal will have all the power of a session court.
(3) The person representing the complainant in Tribunal will be regarded as Public Prosecutor.

51) Opinion of Expert, Training, etc.:-

(1) Tribunal or Appeal Tribunal, while conducting trial, may take independent opinion from an expert in computer science, cyber forensic, electronic communication, data security and other fields.

(2) To implement this Act The government or Agency may, if necessary, provide specialized training to train all people connected to the implementation of the Act in Computer Science, Cyber Forensic, Electronic Communication, Data Security and other necessary fields. .

52) Time Limit for Disposal of Trial:

(1) The adjudicator of the tribunal will dispose of a case under this Act within 180 (one hundred and eighty) working days from the date of the Complaint..

(2) If the adjudicator of the Tribunal fails to dispose of a case within the time limit stated in subsection (1), he can extend the time up to 90 (Ninety) days after recording the reason of such failure.

(3) If the Tribunal Judge fails to dispose of the case within the time limit stated in subsection (2), he will record the reason and bring it to the knowledge of the High Court Division in the form of a report and can continue with the proceedings.

53) Cognizable and Bailable i Offence: -

In this Act-

a. The Offences mentioned in Sections 17, 19, 21, 22, 23, 24, 26, 27, 28, 30, 31, 32, 33 and 34 are cognizable and non-bailable offence; and

b. The Offences mentioned in Subsection (1) , (b) of Section 18, and subsection (3) of Sections 20, 25, 29 and 47 are non-cognizable and bailable.

c. The Offences mentioned in subsection (1) of section 18 are non-cognizable, bailable and can be settled with the permission of the court.

d. In case of a person committing an offence under this Act for the second time or repeatedly, the offence will be cognizable and non-bailable .

54) Confiscation: -

(1) If an offence is committed under this Act then the computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument through which the offence was committed can be confiscated by the order of the tribunal.

(2) Notwithstanding the provision of Subsection (1), if the tribunal is satisfied that the person who was in control or possession of the computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument is not responsible for the offence committed by that instrument, then, the said computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument will not be confiscated.

(3) If the computer, computer system, floppy disk, compact disk, tape drive or any other related computerized materials or instrument fit for confiscation under subsection (1) has any legal computer, computer system, floppy disk, compact disk, tape drive or any other related computer materials or instrument with it, then those instruments will also be confiscated).

(4) Notwithstanding anything contained in this section, if the offence is committed by using any computer or other related computer materials or instrument belonging to a government or constitutional organization then it will not be confiscated.

CHAPTER EIGHT
REGIONAL AND INTERNATIONAL ASSISTANCE

55) Regional and International Assistance:-

If regional or international assistance becomes necessary while conducting an investigation or trial of an offence under this Act, then, the provisions of Crime Related Interpersonal Assistance Act, 2012(Act Number IV of 2012) will be applicable

CHAPTER NINE
MISCELLANEOUS

56) Delegation of Power: -

The Director General may, if necessary, may delegate any power or responsibility entrusted to him under this Act by a written order to any employee of the agency and to any other person or to a police officer.

57) Activities done in good faith:

If a person is harmed or if there is a possibility of being harmed by an activity done while fulfilling a responsibility under this Act, and if the activity is done in good faith, no civil or criminal proceeding or any other legal proceedings can be brought against the employee or person who had responsibility for committing that activity under this Act.

58) Testimonial value:

Notwithstanding anything contained in the Evidence Act 1972 (Act I of 1872), or any other law, any forensic evidence obtained or collected under this Act shall be treated as evidence in the trial proceedings.

59) Removal of Difficulty:

If any ambiguity is noticed while implementing the provisions of this Act, the government may take necessary measures to remove the difficulties, by means of an order published in the official gazette.

60) The power to make rules:-

(1) To fulfil the objective of this Act, government**,** by notification in the government gadget can enact rules.

(2) Without prejudice to the subsection (1), government, by notification in the government gadget, can enact rules for especially for the following among other subjects Namely:-

a. Establishing Digital Forensic Lab;
b. Supervision of the Digital forensic Lab by The Director General
c. Reviewing traffic data or information and the process of its collection and preservation.
d. Process of Interference, Review or Decryption and Protection
e. Security of Compromised Information Infrastructure
f. The process of Regional and International Assistance in terms of Digital security.

g. Creation and operation of Emergency Response Teams and the process of coordination of it with other teams.
h. Cloud Computing, Metadata; and
i. Security of preserved Data

61) The Amendment and Custody of Act No 39 of the year 2006:-

(1) As soon as this Act comes into effect, the sections 54 55 56 57 66 of the Information and Communication Technology Act 2006 (Act no 39 of 2006) will be abolished; henceforth it shall be mentioned that the above enumerated sections of Information Communication Technology Act 2006 has been abolished by this Section.

(2) If any proceedings is initiated or received in the tribunal under the abolished sections or if a case is pending at any stage of the trial process in relation to the abolished sections they will continue as if the sections were not abolished.

62) Publishing of translated text of the Act in English:-

(1) After the Act comes into force, the Government can publish an authentic English text translation of this Act by notification in the official Gazette.

(2) In the case of conflict between Bengali and English text of the Act, the Bengali text will prevail

OBJECTIVE AND REASON CONTAINING STATEMENT

The announced vision 2021 by Prime Minister Sheikh Hasina: in the aim creating digital Bangladesh the usage of data and information technology to its highest is a must. In the present world benefitting by the vast usage of information technology has also increased the wrong application, for which the level of cyber crime is also increasing. In this circumstances, to ensure the national digital security and redress, prevention, identificationand restraint and judgement of digital crimes this Act implementation is a must. To secure the nation and the public life and property from Cyber cum digital crime is the main objective if this Act.

The implementation of digital Bangladesh can be considered as the revival of the Golden Bangladesh of the father of the nation Sheikh Mujibur Rahman. The great dreamer has given his own suitable successor to fulfill the dream of Golden Bangladesh, Honorable Prime Misnister Sheikh Hasina. Digital security Act 2018 will play a helpful role in implementing Vision 2021; Digital Bangladesh.

MUSTAFA JABBAR
MINISTER INCHARGE

BANGLADESH NATIONAL PARLIAMENT

NATIONAL DIGITAL SECURITY CONFIRMATION AND DIGITAL CRIME IDETIFICATION

PREVENTION, RESTRAINT, JUDGMENT AND OTHERS SUBJECTS RELATED PROPOSED BILL FOR FORMULATION AND CONTAINING PART

RECOMMENDATION WAS FOUND FOR THIS THIS BILL ACCORDING TO THE PARAGRAPH 82 OF THE CONSTITUTION

DR. MD. ABDUR ROB HAOLADAR
SENIOR SECRETARY

(MISTER MOSTAFA JOBBAR)

RECOMMENDATIONS OF PERMANENT COMMITTEE POSTAL, TELECOMMUNICATION AND INFORMATION TECHNOLOGY MINISTRY

NAME OF BILL: DIGITAL SECURITY BILL, 2018

Postal, telecommunication and Information technology Ministry related permanent committee correction recommendations in the followings after testing the digital security bill 2018, such as:-

1. **Instead of the long title the following heading will be installed.**

   "TO FORMULATE PROVISIONS ENSURING THE DIGITAL SECURITY AND CRIME IDENTIFICATION, PREVENTION, RESTRAINMENT, JUDGEMENT AND OTHER RELATED SUBJECTS, COMMITTED THROUGH DIGITAL MEDIUM."

2. **The following proposal will be installed instead of the proposal of the Bill, such as:-**

   "SINCE IT IS NECESSARY AND EXPEDIENT TO IMPLEMENT PROVISION TO IDENTIFY, PREVENT, RESTRAINT AND JUDGE THE CRIME OCCURING THROUGH DIGITAL MEDIUM AND TO ENSURE DIGITAL SECUIRTY."

3. On the Section number 2 of the sub-Section (1), will be renumbered as serial number (u) and serial number (v), and thus serial number (t) serial number (u) shall be inserted in the following way. Such as:-

   "(u) ""Cognition of Liberation War", meaning the great ideals who inspired our hero public to dedicate themselves and to sacrifice the life of the hero martyrs. The ideal of those nationalism, socialism, democracy and secularism".

4. **(TEXT WAS CLEAR)**

5. **Before the mentioned word" Digital Security Agency" in The sub-Section(1) of Section 5, by combining a 1(one) director general and 2(two) director, " words and coma has to be insterted.**

6. **The following will be inserted as Section (6) instead of the Section (6) in the bill, such as:-**

   "6" The appointment, period of Director General and Director, etc.:-
   (1) The Director General and the directors will be an expert on computer or cyber security, he will be appointed by the government and the conditions of their job shall be decided by the government.
   (2) The director general or the directors will be the fulltime employee of the agency and for the favour this Act and its provisions, he has perform his activities, use the power and fulfill the responsibilities as per the order passed by the government.
   (3) If the post of the director general is vacant, or if he is absent or sick or for any other reason if he is unable to perform his duties then until the new director general takes charge in the vacant

position or until the director general is capable of joining the responsibilities the eldest director shall fulfill the responsibility of the director general temporarily.

7. In the sub-Section (2) of Section 8, before abbreviating the mentioned word “BRTC” the words and comas will be inserted by the director general.
8. Section 12 of the bill-
    a. Of Sub-Section-
        (i) In serial (b),after the mentioned word “ state minister” , the sign and the word “deputy minister” is to inserted;
        (ii) The serial (c) number will be inserted as new serial of serial number (b) and thus the immediate numbers will (c), (d), (e), (f), (g), (h), (i),(j), and (k), hence the serials shall be renumbered as (c), (d), (e), (f), (g), (h), (i),(j), and (k).

    b. Tin Sub-Section (3), the mentioned “as a member of it any suitable representative of intuitions, etc. at any time by considering the agenda of the meeting temporarily may co-opt. “instead of those words and the bracket, “or by the recommendation of the information ministry1 (one) representative can be the member and can co-opt any time,” these words and coma will be inserted.
9. The mentioned “1(one) year” in Section 18, sub-Section (2), serial number (a) of the bill, instead of the number, bracket and the words, “6(six) months” number, bracket and the words and instead of “3(three) lacs” number, bracket, words, “2(two) lacs “ number, bracket and words shall be inserted.