LAW Related Questions and Answers

Made by Md. Mehedi Hasan Rafy

Cyber Security Act 2023

Definition

Appellate Tribunal

"Appellate Tribunal" means the Cyber Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006);

Data storage

"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;

Computer system

"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;

Critical information infrastructure

"Critical information infrastructure" means any external or virtual information infrastructure declared by the Government those controls, processes, circulates or preserves any information-data or digital or electronic information and, if damaged or critically affected, may adversely affect—

(i) public safety or financial security or public health; and

(ii) national security or national integrity or sovereignty

Tribunal

"Tribunal" means the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006);

Digital device

"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;

Malware

"Malware" means such kind of computer or digital instruction, data information, program 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;

(ii) being connected with any other computer or digital device, becomes auto-active while activating any program, 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; or

(iii) creates opportunity of stealing information from a digital or electronic device or automatic access to it;

Cyber security

"Cyber security" means the security of any digital device, computer or computer system;

Application of the Act

(1) If any provision of any other law is inconsistent with any provision of this Act, the provision of this Act shall apply to the extent inconsistent with the provision of that any other law.

(2) Notwithstanding anything contained in sub-section (1), the provisions of the Right to Information Act, 2009 (Act No. 20 of 2009) shall be applicable to a matter related to right to information.

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, computer network or digital device 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.

Power to remove or block some data-information

(1) If any data information related to any matter under the jurisdiction of the Director General, being published or propagated in digital or electronic media, creates threat to cyber security, the

Director General may request the Bangladesh Telecommunications and Regulatory Commission, hereinafter referred to as BTRC, to remove or, as the case may be, block the said data-information.

(2) If the law and order enforcing force, subject to the analysis of information and data, has reasons to believe that any data-information published or propagated in digital or electronic 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.

Emergency Response Team

(1) For carrying out the purposes of this Act, there shall be a National Computer Emergency Response Team under the Agency.

(2) Any critical information infrastructure declared under section 15 may, if necessary, form its own Computer Emergency Response Team or Computer Incident Response Team, with the prior approval of the Agency.

(3) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall consist of the persons expert in cyber security and, if necessary, members of law-and-order enforcing force.

(4) The National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge duties in such manner as may be prescribed by rules, on full time basis.

(5) Without prejudice to the generality of sub-section (4), the National Computer Emergency Response Team and the Computer Emergency Response Team or the Computer Incident Response Team shall discharge the following duties, namely: —

(a) to ensure the emergency security of the critical information infrastructure;

(b) to take immediate necessary measures for remedy if there is any cyber or digital attack and if the cyber or digital security is affected;

(c) to take necessary initiatives for preventing 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 approval of the Government; and

(e) to do such other acts as may be prescribed by rules.

(6) The Agency shall supervise and make co-ordination amongst the National Computer Emergency Response Team, the Computer Emergency Response Teams or Computer Incident Response Teams.

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 organization 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 labs 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 labs shall be prescribed by rules.

Functions of digital forensic labs

(1) The Agency shall ensure the quality of each digital forensic lab according to the standards prescribed by rules.

(2) In case of ensuring the quality prescribed under sub-section (1), each digital forensic lab shall, inter alia, —

(a) operate the functions of the lab by properly qualified and trained manpower;

(b) ensure its physical infrastructural facilities;

(c) take necessary initiatives to maintain the security and secrecy of the data-information preserved thereunder;

(d) use quality instruments in order to maintain the technical standard of the digital forensic test; and

(e) perform its functions following scientific method in such manners as may be prescribed by rules.

Establishment of National Cyber Security Agency

(1) For carrying out the purposes of this Act, the Government shall, by notification in the official Gazette, establish an Agency to be called the National Cyber Security Agency consisting of 1 (one) Director General and such number of Directors as may be prescribed by rules.

(2) The head office of the Agency shall be located in Dhaka, but the Government may, if necessary, set up its branch office at any place in the country outside of Dhaka.

(3) The Agency shall administratively remain as attached office with the Information and Communication Technology Division.

(4) The powers, responsibilities and functions of the Agency shall be prescribed by rules.

Power of the National Cyber Security Council

(1) For implementation of the provisions of this Act and the rules made thereunder, the Council shall give necessary direction and advice to the Agency.

(2) The Council shall, inter alia, perform the following functions, namely: —

(a) to provide necessary directions for remedy if cyber security is under threat;

(b) to give advice for infrastructural development of cyber security and enhancement of its manpower and quality;

(c) to formulate inter-institutional policies to ensure the cyber security;

(d) to take necessary measures to ensure the proper application of this Act and rules made thereunder; and

(e) to do such other act as may be prescribed by rules

Digital or electronic forgery

(1) If any person commits forgery by using any digital or electronic medium, such act of the person shall be an offence.

(2) If any person commits an offence under sub-section (1), he shall be punished with imprisonment for a term not exceeding 2 (two) years, or with fine not exceeding Taka 5 (five) lakh, 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 authorized right or by means of unauthorized practice, erroneous data or program, information or wrong activity, information system, computer or digital network by producing, changing, deleting and hiding input or output of any computer or digital network by a person.

Digital or electronic fraud

(1) If any person commits fraud by using any digital or electronic medium, 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) lakh, 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 program, computer system, computer network, digital device, digital system, digital network or social media by a person, intentionally or knowingly or without permission, and by 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.

Cyber defamation

(1) If any person publishes or transmits any defamatory information as described in section 499 of the Penal Code (Act XLV of 1860) in website or in any other electronic format, then such act of the person shall be an offence, and for this reason, he shall be punished with fine not exceeding Taka 25 (twenty-five) lakh.

Hacking and punishment

If any person commits hacking, it shall be an offence, and for this, he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both.

Explanation: For the purposes of this section,"hacking" means—

(a) to steal, 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.

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 program, computer system or computer network, or tries to hide, damage or modify the source code, program, system or network through another person, and if such source code is preservable or maintainable, 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) lakh, or with both.

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

(1) If any person, through any website or any other digital or electronic medium—

(a) intentionally or knowingly transmits, publishes or propagates any data-information which he knows to be offensive, false or threatening in order to annoy, insult, humiliate or malign a person; or

(b) publishes or propagates or abets to publish or propagate any information, as a whole or partly, which he knows to be propaganda or false, with an intention to affect the image or reputation of the country, or to spread confusion, then such act of the person shall be an offence.

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

Disclosure of confidentiality and privacy

(1) If any person collects, sells, possesses, provides or uses identity information of any other person without lawful authority, such act of the person shall be an offence.

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

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, with an intention to hurt or provoke the religious values or sentiments, 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, such act of the person shall be an offence.

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

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;

(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 any other foreign country or public order, or may be used for the benefit of any foreign country or any individual or any group, then such act of the person shall be 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

Investigation

(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 it is necessary to form an investigation team for fair investigation, 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 on such condition as may be referred to in the order.

ICT Act 2006

Definition

Digital signature

"Digital signature" means data in an electronic form, which--

(a) is related with any other electronic data directly or logically; and

(b) is able to satisfy the following conditions for validating the digital signature--

(i) affixing with the signatory uniquely;

(ii) capable to identify the signatory;

(iii) created in safe manner or using a means under the sole control of the signatory; and

(iv) related with the attached data in such a manner that is capable to identify any alteration made in the data thereafter.

Electronic gazette

"electronic gazette" means the official gazette published in the electronic form in addition to official printed & published gazette;

Internet

"Internet" means such an international computer network by which users of computer, cellular phone or any other electronic system around the globe can communicate with one another and interchange information and can browse the information presented in the websites.

Website

"Website" means document and information stored in computer and web server which can be browsed or seen by the user through internet;

Computer

"Computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

Computer Network

"Computer network" means the interconnection of one or more computers through the use of satellite, microwave, terrestrial line, wireless equipment, wide area network, local area network, infrared, Wi-Fi, Bluetooth or other communication media; and terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

Power of Government to make rules in respect of digital signatures

The Government may, by notification in the Official Gazette and in additionally optionally in the Electronic Gazette, make the following rules (all or any of them) to prescribe for the purposes of this Act-

(a) the type of digital signature;

(b) the manner and format in which the digital signature shall be affixed;

(c) the manner and procedure which facilitates identification of the person affixing the digital signature;

(d) the control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records and payments; and

(e) any other matter which is necessary to give legal effect to digital signatures

Revocation of Digital Signature Certificate

A Certifying Authority shall revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub-section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's identification/security system was compromised in a manner materially or as a whole affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent by a competent court or authority.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Revocation of Digital Signature Certificate

A Certifying Authority shall revoke a Digital Signature Certificate issued by it—

(a) where the subscriber or any person authorized by him makes a request to that effect; or

(b) upon the death of the subscriber; or

(c) where the subscriber is a firm or a company, if it has been dissolved or wound up or has otherwise ceased to exist.

(2) Subject to the provisions of sub-section (3) of this section and without prejudice to the provisions of sub-section (1) of this section, a Certifying Authority may revoke a Digital Signature Certificate which has been issued by it at any time if it is of opinion that—

(a) a material fact represented in the Digital Signature Certificate is false or has been concealed;

(b) a requirement for issuance of the Digital Signature Certificate was not satisfied;

(c) the Certifying Authority's identification/security system was compromised in a manner materially or as a whole affecting the Digital Signature Certificate's reliability;

(d) the subscriber has been declared insolvent by a competent court or authority.

(3) A Digital Signature Certificate shall not be revoked unless the subscriber has been given an opportunity of being heard in the matter.

(4) On revocation of a Digital Signature Certificate under this section, the Certifying Authority shall communicate the same to the subscriber.

Duties of Subscriber

- **Application of security procedure**.

The subscriber shall apply required security procedure to ensure the purity of Digital Signature Certificate issued by a Certifying Authority.

- **Acceptance of Digital Signature Certificate**

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate to one or more persons or in a repository.

(2) By accepting Digital Signature Certificate, the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that--

(a) all representations made by the subscriber to the Certifying Authority and all materials relevant to the information contained in the Digital Certificate are true; and

(b) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

- **Presumption of represented information of obtaining Digital Signature Certificate**

All material representations made by the subscriber to a Certifying Authority for purposes of obtaining a certificate, including all information known to the subscriber and represented in the Digital Signature Certificate, shall be accurate and complete to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the Certifying Authority.

- **Control of safety measure of subscriber**

(1) Every subscriber shall exercise reasonable care to retain control of using of Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the security of Digital Signature Certificate has been compromised by disobeying the rules in sub-section (1) of this section, the subscriber shall communicate the same without any delay to the Certifying Authority who has issued the Digital Signature Certificate in an agreed manner.

Establishment of Cyber Tribunal

(1) The Government shall, by notification in the Official Gazette, establish one or more Cyber Tribunals to be known as Tribunal at times for the purposes of speedy and effective trials of offences committed under this Act.

(2) Cyber Tribunal established under sub-section (1) of this section in consultation with the Supreme Court shall be constituted by a Session Judge or an Additional Session Judge appointed by the Government; and similarly appointed a Judge to be known as "Judge, Cyber Tribunal."

(3) Local jurisdiction of entire Bangladesh or jurisdiction of one or more Session Divisions can be given to the Cyber Tribunal established under this Act; and the Tribunal only prosecutes the offences committed under this Act.

(4) The on-going prosecution of any case of any Session Court shall not be suspended or transferred automatically to the Tribunal of local jurisdiction concerned due to tendering of local jurisdiction of entire Bangladesh or parts of jurisdiction constituted by one or more Session Divisions to the Tribunal established by the Government later on, however, the Government by notification in the Official Gazette, transfer the case to the Tribunal having special local jurisdiction.

(5) Any Tribunal, taken decision otherwise, shall not be bound to retaking statement of witness who has already given statement, or taking rehearing or begin again any other activities already undertaken under sub-section (1) of this section, however, the Tribunal shall continue the prosecution from where it stood on the basis of already taken or presented statement from the witness.

(6) The Government, by order, shall define the place and time; accordingly the special Tribunal shall conduct its activities from that place and time.

Trial procedure of Cyber Tribunal

(1) Without written report of a police officer not below the rank of Sub-Inspector or the prior approval of the Controller or any other officer authorized by the Controller the special Tribunal shall not accept any offence trial.

(2) The Tribunal shall follow the rules mentioned in the Chapter 23 of the Code of Criminal Procedure, if they are not inconsistent with the rules of this Act, which is used in Session Court.

(3) Any Tribunal shall not suspend any prosecution without having written reasons and unless it is required for the sake of just adjudication.

(4) If the Tribunal is in the opinion that the accused person has been absconded and for that it is not possible to arrest him and produce him before the Tribunal and there is no possibility to arrest him immediately, in that case the Tribunal can order the accused person to appear before the Tribunal by publishing such order in two mass circulated national Bengali dailies and if the accused person fails to do so, the prosecution shall take place in his absence.

(5) The rules mentioned in sub-section (4) of this section shall not be applicable if the accused person fails to appear before the Tribunal or absconded after getting bail.

(6) The Tribunal can order any police officer, or the Controller, or any officer authorized by the Controller, as the case may be, to reinvestigate the case and submit the report within the stipulated time of its own initiative or any application lodged to the Tribunal.

Time limit to deliver verdict

(1) The Judge of Cyber Tribunal shall give the verdict within ten days from the date of completing of taking evidence or debate, what happened later, unless he extends the time limit no more than ten days with having written reasons.

(2) If the verdict is given by the Cyber Tribunal under sub-section (1) of this section or any appeal is lodged against the verdict to the Cyber Appellate Tribunal then Cyber Tribunal or Cyber Appellate Tribunal concerned shall forward the copy of the verdict of the appeal to the Controller for preserving it in the electronic records repository room established under section 18 (7) of this Act.

Investigation of crime

(1) Whatever is contained in the Code of Criminal Procedure, the Controller or any officer authorized by the Controller, or any police officer not below the rank of Sub-Inspector of the Police shall investigate any offence committed under this Act.

(2) Offence committed under this Act shall be non-cognizable offence.

Confiscation

(1) Any computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, or in respect of which any offence has been committed, shall be liable to confiscation by an order of the court trying an offence or contravention.

(2) If the court is satisfied, that the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories belonging to a person or under control of him related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has not been responsible to contravene, or committing an offence, then the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories shall not be confiscated.

(3) If any legal computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories is found with the computer, computer system, floppies, compact disks (CDs), tape drives or any other accessories which is confiscated under sub-section (1) of this section shall also be confiscated.

(4) Any computer or other relevant accessories belonging to the Government or Body Government Authority is used to commit an offence under sub-section (1) of this section, whatever contained in this section, shall not be confiscated.