IN THE NAME OF ALLAH, THE GREATEST THE MOST MERCIFUL

# INTERNATIONAL ISLAMIC UNIVERSITY CHITTAGONG

## Department of Electronic and Telecommunication Engineering

## CT- 2

| | |
|---|---|
| **Matric / ID No** | **T181056** |
| **ID No. (In Words):** | **T-One Eight One Zero Five Six** |
| **Name** | **Soumen Barua** |
| **Semester / Trimester** | **Spring** |
| **Academic Year** | **2021** |
| **Program** | **Bachelor of Science (B.Sc.)** |
| **Course Code** | **Law 4721** |
| **Course Title** | **Professional Ethics and Environmental Protection Law** |
| **Course Teacher Name** | **Mohammadullah Mojaher (Advocate)** |
| **Semester Enrolled** | **7th** |
| **Section** | **B** |
| **Email ID** | **b.soum3n@gmail.com** |
| **Contact Number** | **01629188979** |

| **Submitted To:** | | **Remarks:** |
|---|---|---|
| **Name** | **Mohammadullah Mojaher (Advocate)** | |
| **Designation** | **Adjunct Faculty,** | |
| **Department** | **Dept. of Law** | |
| **Institution** | **IIUC** | |

**Signature of Examiner**

# The Digital Security Act 2018

**1. Background of this Law:** Throughout the history of mankind man has continuously adapted his way of life in function of the technology that he has, as defined "man is man and his circumstance". As civilization evolves to grow increasingly connected through the inevitable ubiquity of technology, securing systems, networks and data on which we rely on has become paramount.

Cybercrime is a major threat for economics, individual safety and even the public in general, as it is a primary medium for terrorism. Global cyber security has been increasing in our society, and represents a variety of threats at the level of companies, individuals or governments. The evolutions of the technologies have led to an increase of the social networks, accentuated in recent times as a result of the development of the technology. Security, privacy, and attack-free communication can lead to an optimal and realistic healthcare system. To ensure attack-free communication in remote healthcare systems, there must be some countermeasures to protect the data and detect any intrusions in the human personal data during wireless communications in healthcare systems.

The proximity of technologies to rehabilitation has been accentuated in recent times as a result of technological development. Today our society is in transformation, with the growing influence of existing technology. People increasingly focus their attention on new technologies, exposing themselves by sharing personal information and confidential data, making them more and more accessible to attack. After you connect to the Internet, you lose your 100% safety humanity evolves rapidly as the growth of public accessible knowledge has been greatly nurtured and facilitated.

In trying to make a law to prevent crimes through digital devices and provide security in the digital sphere the Act ends up policing media operations, censoring content and controlling media freedom and freedom of speech and expression as guaranteed by our constitution.

The Act gives unlimited power to the police to enter premises, search offices, bodily search persons, seize computers, computer networks, servers, and everything related to the digital platforms. According to the Act, the police can arrest anybody on suspicion without warrant and do not need any approval of any authorities.

In the present world benefitting by the vast usage of information technology has also increased the wrong application, for which the level of cybercrime is also increasing. In this circumstance, to ensure the national digital security and redress, prevention, identification and restraint and judgement of digital crimes this Act implementation is a must. One of the main objectives of the proposed law is to ensure the country's security from digital crimes and ensure security of people's lives and assets.

**2. Offences and punishments**

Sections 17 to 38 of the bill present in parliament outlines the following offences and punishments

- One may face 7 years jail or 2.5 million Tk in fines, or both, for entering important information infrastructure illegally.
- Intrusion into important information infrastructures and destruction or attempts to destroy information carry up to 14 years jail or 10 million Tk in fine, or both.
- The bill has a provision of 1 year jail or Tk 300,000 in fines or both in case of illegal entry to a computer or digital device.
- A person may face up to 3 years jail or Tk 1 million in fines or both for assisting in illegal entry to a computer or digital device.
- The new bill also includes a provision of 7 years in jail or Tk 1 million in fines or both if data, information, or its copies are illegally collected or transferred from a computer or computer system.
- A person may face 3 years in jail or a Tk 300,000 in fine in case of destroying or changing computer source code.
- Any person spreading 'negative propaganda' against the Liberation War, the spirit of the Liberation War or the Father of the Nation or assisting in its spread on digital media may face 14 years jail or Tk 10 million in fines or both.
- The bill includes provision of 5 years jail or Tk 500,000 in fines, or both, for any case of forgery or cheating using the digital or electronic medium.
- A person will be considered a 'cyber-criminal' if they create a hindrance to the legal entry to any computer or internet network or assist in the process in order to create panic among people or to attack the integrity, security and sovereignty of the state and may face 14 years of jail or 10 million Tk in fine or both.
- A person may face 7 years in jail or a Tk 1 million fine or both if they publish or broadcast something offensive to religious sentiments and values or make others to do so on a website or electronic medium.
- If a person commits a defamation offence on website or other electronic medium under section 499 of the Penal code, they will face up to 3 years jail or Tk 500,000 in fines or both.
- A person who deliberately broadcasts or posts in an attempt to s spread enmity and hatred among a concerned class or community, deteriorates law and order or destroys communal harmony, or makes others do so on a website or digital medium may face up to 7 years jail or Tk 500,000 in fines or both.
- The bill has a provision of 5 years jail or Tk 500,000 in fines or both in cases where anyone conducts an online transaction without legal authority using electronic or digital medium with any bank, insurance agency or other financial service providing organization.
- Any person sending 'attacking' or 'frightening' information through a website or other digital medium may face up to 3 years in jail or Tk 300,000 in fine or both.
- Any act of recording, sending or preserving information, data from a government, semi-government, autonomous organisation or a statutory body through computer, digital device, digital network or any other electronic media or providing assistance to the act will be considered as 'spying' and may lead to a sentence of l up to 14 years in jail or Tk 2.5 million in fines, or both.

- A person can get 14 years in jail or Tk 10 million in fines or both for hacking.

## 3. Trial Procedure

### Investigation

According to the section 39 Police Officer, hereinafter mentioned as the investigation officer in this chapter, will investigate offence committed under this Act. 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.

### Time limit of Investigation

According to the section 40 Investigation officer shall complete the investigation within 60 days from the date of getting charge of the Investigation. 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. 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. 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.

### Power of Investigation Officer

According to the section 41 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.

### Search and Seizure through Warrant

According to the section 42 If any police office has reason to believe that, or an offence has been committed or there is possibility of commission of an offence under this Act, orb. 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 to seize any traffic data which is under possession of any service provider, At

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

**Search, Seizure and Arrest without Warrant**

According to the section 43 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: Enter and search the said place and, if interrupted, take necessary action in accordance with the Code of Criminal Procedure;

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; Conduct physical search of any person present in that place; Arrest anyone present in the said place if suspected of committing or having committed an offence under this Act. After conducting a search under subsection (1), the police officer will submit a search report to the Tribunal.

**Secrecy of the Information obtained in the Investigation:**

According to the section 47 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. All person, entity or service provider related with the investigation under this Act shall maintain secrecy of information related to the investigation. 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

**Cognizance of Offence:**

According to the section 48 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. 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.

**Adjudication of Offence and Appeal:**

According to the section 49 notwithstanding provisions of any other law that are currently in force, offence committed under this Act will be tried by the Tribunal exclusively. Any person aggrieved by the judgment of the tribunal may appeal in the Appeal Tribunal.

**Application of forgery code of conduct: -**

According to the section 50 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. 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. The person representing the complainant in Tribunal will be regarded as Public Prosecutor.

**Opinion of Expert, Training, etc.:**

According to the section 51 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. 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.

**Time Limit for Disposal of Trial:**

According to the section 52 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. 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. 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.

**Cognizable and billable Offence:**

According to the section 53 in this Act. 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 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. The Offences mentioned in subsection (1) of section 18 are non-cognizable, bailable and can be settled with the permission of the court. 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.

**Confiscation**:

According to the section 54 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. 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.

If the computer, computer system, floppy disk, compact disk, tape drive or any other relate 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). 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.