4 January:

Ict law বাংলাদেশ এ দুইটি specific আইন রয়েছেঃ

১। digital security act 2018

২। Information & Communication Technology Act, 2006

ICT law এর ক্ষেত্রে ডিজিটাল medium টা গুরুত্তপূর্ণ (mobile, মেমোরি কার্ড,pendrive, internet). ডিজিটাল medium যদি না থাকে তবে Ict law applicable হবে না.

ignorance of law is not an excuse.

2 types of offence হয়, 1টা civil and আরক টা criminal.

Civil : জমি জমা , পারিবারিক বাপার, personal metters(divorce), etc.

আমরা যেটা পরছি সে টা criminal offence. Criminal case এ jail or জরিমানা or both will apply.(যদি কোন আইন এর মধ্যে jail থাকে তবে তা অবশ্যই criminal offence)

Q. এ ঘতনা দেয়া থাকবে। Ans আমকে সেখানে বলতে হবে যে সে অপরাধ টা করেছে কি করে নাই. যদি বলি যে সে অপরাধ টা করেছে তবে আমকে এতাও বলতে হবে যে , এই অপরাধ এর কারনে ..... এই ধারায় under e সে এই শাস্তি টা পাবে।

ত এটা করার জন্য আমকে ২টা জিনিস প্রমান করতে হবে।

element of crime→ প্রমান করতে হবে ACTUS REAS এর মাদ্ধমে ।

mental element→ প্রমান করতে হবে MENS REA এর মাদ্ধমে (Intension and knowledge)

1.ACTUS REAS(কাজ): আপনার কাজের সাথে সম্পর্কযুক্ত, আপ্নে কাজ তা করেছেন, এবং আপনার কাজ টার করার মাদ্ধমে element of crime(উপাদান= element of crime) (উপাদানঃ আপনার ঘরে সে প্রবেস করল -১টা উপাদান, বিনা অনুমতি তে কিছু পকেটে ঢুকাল-২য় উপাদান-চুরি করল সে) এই উপাদান গুলা যদি আমি দেখাইতে পারি (Q. এ যে ঘটনা দেয়া হয়েছে টার মধ্যে section অনুযাই সব উপাদান গুলাই আছে) তাহলে ACTUS REAS proved

2.MENS REA(mental element): Criminal offence খালি কাজ করলে হই না। criminal offence এর জন্য তাকে এটাও প্রমান করতে হবে যে টার কাজ টি করার উদ্দেস্য ছিল, এবং টার এই সম্পরকে গ্যান ছিল।(Intension and knowledge)

Now: Information and Communication Technology Act, 2006 (OPEN):

Act No. 39 of the year 2006

Act prepared to provide legal recognition and security of Information and Communication Technology and rules of relevant subjects

Since it is plausible and necessary to provide legal recognition and security of Information & Communication Technology and prepare rules of relevant subjects;

Thus hereby the following Act has been created:--

Chapter I
PRELIMINARY

1. Short Title, extent and commencement.--(1) This Act may be called the Information & Communication Technology Act, 2006.

(2) It shall extend to the whole of Bangladesh.

2. Definitions.-- In this Act, unless the context otherwise requires,--

(1) "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.

"**Act No. 39 of the year 2006**" means: 39th act of 2006, before this act 38 acts have passed in the parliament in 2006.

Chapter I
PRELIMINARY

1. Short Title, extent and commencement.--(1) This Act may be called the Information & Communication Technology Act, 2006.

(2) It shall extend to the whole of Bangladesh.

2. Definitions.-- In this Act, unless the context otherwise requires,--

(1) "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

Inside **section** there is another 1,2 or more numbers, these are **subsection**.
Inside **subsection** there are a,b,c. these are **clause**.
Inside a,b,c we see i, ii, ii, iv . these are **sub clause**.
Section1 of a act always contain the sort title of an act.

Bangladesh National Parliament

Dhaka, 23 Ashwin, 1413/8 October, 2006

The following Act undertaken by the Parliament received approval from the President on 23 Ashwin, 1413 corresponding to 8 October 2006 and thus published for the public: --

Act No. 39 of the year 2006

Act prepared to provide legal recognition and security of Information and Communication Technology and rules of relevant subjects

Since it is plausible and necessary to provide legal recognition and security of Information & Communication Technology and prepare rules of relevant subjects;

Thus hereby the following Act has been created:--

Chapter I
PRELIMINARY

Long title পরে আমরা যা বুঝতে পারিঃ act টা create করা হয়েছে legal recognition and security দেয়ার জন্য।(কেউ কোন software or app তৈরি করলে তার legal recognition and security দেয়ার জন্য এই act create করা হইয়েছে, এবং অগুলর উপর প্রয়জনিয় নিয়ম কানুন প্রয়োগ করার জন্য ও এই act create করা হয়েছে)

Now, section 57 of Information and Communication Technology Act, 2006:

“

57. Punishment for publishing fake(মিথ্যা), obscene(অশ্লীল) or defaming(মাণহাণী)(৩ টার যেকোনো ১ টা হলেই punishment) information in electronic form.—>

(1) If any person deliberately(ইচ্ছাকরে) **publishes or transmits or causes** to be published or transmitted in the website or in electronic form any material which is **fake and obscene or its effect is such**(১,২ offence) as to tend to **deprave(৩offence, নৈতিকতা নষ্ট) and corrupt(4offence, দুর্নীতি গ্রস্থ)** persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, or causes to **deteriorate or creates possibility(5offence)** to deteriorate law and order, **prejudice the image(6offence)** of the State or person**(7offence)** or **causes to hurt(8offence)** or may hurt religious belief or instigate against**(9offence)** any person**(10offence)** or organization, then this activity of his will be regarded as an offence.

(2) Whoever commits offence under sub-section (1) of this section he shall be punishable with imprisonment for a term which may extend to ten years and with fine which may extend to Taka one crore.

”

Here in subsection ‘2’ ১০ বছর jail এর জায়গায় ১৪ বছর হবে।
Digital security act, 2018 এর মাদ্ধমে এই Information and Communication Technology Act, 2006 এর section 57 বাতিল করা হয়েছে।(অনেক গুলা section এর মধ্যে এই Information and Communication Technology Act, 2006 এর section 57 কে ভাগ করে দেয়া হয়েছে) (total 10 offence)

10 January:

Act No. 39 of the year 2006

Act prepared to provide legal recognition and security of Information and Communication Technology and rules of relevant subjects

Since it is plausible and necessary to provide legal recognition and security of Information & Communication Technology and prepare rules of relevant subjects;

Thus hereby the following Act has been created:--

Chapter I
PRELIMINARY

1. Short Title, extent and commencement.--(1) This Act may be called the Information & Communication Technology Act, 2006.

(2) It shall extend to the whole of Bangladesh.

2. Definitions.-- In this Act, unless the context otherwise requires,--

(1) "digital signature" means data in an electronic form, which--

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

Information & Communication Technology Act, 2006 এর section 1 এর সুব সেচতিওন 2 হলঃ

Jurisdiction অথবা এখতিয়ার (এটা কে territorial jurisdiction ও বলা হয়ে থাকে) অর্থাৎ এই act এর বাপ্তি কত তা বুঝায়। বাংলাদেশ এর মধ্যে যা কিছু ঘটবে এই act এর অধিনে যদি অপরাধ হয়ে থাকে তাহলে টার উপরে এই আইন applicable হবে। অর্থাৎ যদি কেও কাওকে digital media তে defame করে এবং সে যদি তা বাংলাদেশ এর ভিতরে বসে সেটা করতে থাকে তাহলে এই আইনে যে শাস্তি দেয়া আছে তাকে ধরতে পারলে সেই শাস্তি court দিবে।

Now in, **Digital Security Act, 2018 এর:**

Territorial jurisdiction না থাকা কোন act er বড় রকম এর অপুরনতা(ঘারতি)

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

→ No jurisdiction

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

[Q. discuss the conflicting provision of Information & Communication Technology Act, 2006 and Digital Security Act] [create a fact]

Now, **Information & Communication Technology Act, 2006 এর section 3:**

“

3. Domination of the Act.—

Where any law provides whatever anything it contained, the rules of this Act shall be in force;

” অন্য যে আইনে যা ইচ্ছা বলা থাকুক, এই আইন ইই সব সমই বলগত থাকবে।

On the other hand : in Digital Security Act, 2018 এর section 3

“

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

“

অর্থাৎ এই আইন সব সময় প্রধান্ন পাবে, তবে যদি The Right to Information Act 2009 এর সাথে conflict করে তবে The Right to Information Act 2009 প্রাধান্ন পাবে।

যেমনঃ The Right to Information Act 2009 says that NSI(national security force) can disagree to give any information, but if digital security act says that they can ask for information to any one, then The Right to Information Act 2009 will apply.

Again on the other hand : **Information & Communication Technology Act, 2006 এর section 3:**

“

3. Domination of the Act.—

Where any law provides whatever anything it contained, the rules of this Act shall be in force;

" তাহলে **Information & Communication Technology Act** অনুজায়ি সকলে তথ্য দিতে বাধ্য(including NSI)

Section 4 ICT act, 2006:

"

4. Inter-state application of the Act.—(অন্তঃরাষ্ট্রিয় প্রয়োগ)(এই আইন এর মাদ্ধেঃ একজন Indian পাকিস্তান এর বিরুদ্ধে অপরাধ যেমন hacking, করলেও তা অপরাধ)

(1) If **any person** commits offence or contravention(অমান্ন করা) under this Act **outside of Bangladesh,** which is punishable under this Act if he commits it in Bangladesh, then this **Act shall apply as such he commits offence or contravention in Bangladesh**;

(2) If any person commits offence or contravention in Bangladesh under this Act from outside Bangladesh using a computer, computer system or computer network located in Bangladesh, then this Act shall apply as such the entire process of the offence or contravention took place in Bangladesh; (দেশের বাহিরে বসে কোন হ্যাকার দেশের ভিতরের কোন ক্ষতি করলে তা দেশের ভিতরে ঘটেছে বলে ধরে নেয়া হবে)

(3) If any person from within Bangladesh commits offence or contravention outside of Bangladesh under this Act, then this Act shall apply against him as such the entire process of the offence or contravention took place in Bangladesh;(দেশে বসে কোন হ্যাকার বাহিরের দেশের কোন ওয়েবসাইট হ্যাক করলেও তা অপরাধ)

"

Now,

Digital Security Act, 2018 এর section 4:

"

4. Extra territorial application of the Act.— (same as section 4, ICT act, 2006)

(1) If any person commits any offence under this Act beyond Bangladesh which would be punishable under this Act if committed in Bangladesh, the provisions of this Act shall be applicable in such manner as if he had committed such offence in Bangladesh.

(2) If any person commits any offence within Bangladesh under this Act from outside of Bangladesh using any computer, computer system, or computer network situated in Bangladesh, the provisions of this Act shall be applicable to the person in such manner as if the whole process of the offence had been committed in Bangladesh.

(3) If any person commits any offence beyond Bangladesh under this Act from inside of Bangladesh, the provisions of this Act shall be applicable in such manner as if the whole process of the offence had been committed in Bangladesh.

"

11 January:

At first try to recap the target(উদ্দেশ্য) of the act: **(Digital Security Act, 2018)**

Provisions=প্রতিরোধ

Suppression=দমন

Trail= বিচার

Act:

DIGITAL SECURITY ACT, 2018

Act No. XLVI of 2018

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

Now,

প্রতিষ্ঠান গুল পড়বোঃ Digital Security Act, 2018 এর অধিনে বেস কিছু প্রতিষ্টান আছে, জেগুল আসলে Digital Security Act, 2018 এর যে উদ্দেশ্য সে উদ্দেশ্য পুরনে সহায়তা করে।

তার মধ্যে ১ম যে প্রতিষ্টান হল digital security agency.

In **Digital Security Act, 2018: section2 subsection 1 clause (C):**

“

(c) “Agency” means the Digital Security Agency established under section 5 of this Act;

“তার মানে section 5 এ বলে দিয়েছে যে কিরকম করে agency তৈরি হবে

In **Digital Security Act, 2018: section2 subsection 1 clause (d):**

“

(d) “Computer Emergency Response Team” means the National Computer Emergency Response Team or Computer Emergency Response Team formed under section 9;

“ Computer Emergency Response Team কারা, বলছে তারা যাদের কিনা এই act এর section 9 এর অধিনে যে National Computer Emergency Response Team(এটা এক টায় হয়, সবার মাথার উপরে, এর অধিনে আর থাকতে পারে) অথবা Computer Emergency Response Team গঠন করা হয়েছে সেটা কে বুঝানু হয়েছে।

In **Digital Security Act, 2018: section2 subsection 1 clause (f):**

“

“Council” means the **National** Digital Security Council constituted under **section 12;**

”

Now In Digital Security Act, 2018: section5:

“

5. Establishment of Agency, Office, etc. (agency তৈরি হয়েছে Digital Security Act এর উদ্দেশ্য পুরন এর জন্য)

(1) For carrying out the purposes of this Act, the Government shall, by notification in the official Gazette, establish an Agency to be called the Digital Security Agency consisting of **1 (one) Director General** and **2 (two) Directors**.

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

(3) The powers, responsibilities and functions of the Agency shall be prescribed by **rules.** (rules parliament এ পাস হতেও পারে নাও পারে, rules can be passed by the executive, rules are not considered as parliamentary act, so when the rules are made outside the parliament the democracy is compromised, because they are made by the excitative not by the Public representative)

“

Now In Digital Security Act, 2018: section6:

“

6. Appointment of the Director General and the Directors, tenure, etc.

(1) The Director General and the Directors shall be appointed by the Government from among the persons specialist in computer or cyber security, and the **terms and conditions** of their service shall be determined by the **Government**.

(2) The **Director General** and the **Directors** shall **be full time employees of** the Agency and shall, subject to the provisions of this Act and rules made thereunder, perform such functions, exercise such powers and discharge such duties as may be directed by the Government. (সরকারের ক্ষমতার অপব্যবহার করার সুযোগ থাকছে, There is an opportunity to abuse the power of the government, as everything is managed by the government)

(3) If a vacancy occurs in the office of the Director General, or if the Director General is unable to perform his duties on account of absence, illness or any other cause, the senior most Director shall provisionally perform the duties of the Director General until the newly appointed Director General assumes his office or the Director General is able to resume the functions of his office.

“

৬। **মহাপরিচালক ও পরিচালকগণের নিয়োগ, মেয়াদ, ইত্যাদি।**—(১) মহাপরিচালক ও পরিচালকগণ, কম্পিউটার বা সাইবার নিরাপত্তা বিষয়ে বিশেষজ্ঞ ব্যক্তিদের মধ্য হইতে, সরকার কর্তৃক নিযুক্ত হইবেন এবং তাহাদের চাকরির শর্তাদি সরকার কর্তৃক নির্ধারিত হইবে।

(২) মহাপরিচালক ও পরিচালকগণ এজেন্সির সার্বক্ষণিক কর্মচারী হইবেন, এবং তাহারা এই আইন এবং তদধীন প্রণীত বিধির বিধানাবলি সাপেক্ষে, সরকার কর্তৃক নির্দেশিত কার্য-সম্পাদন, ক্ষমতা প্রয়োগ ও দায়িত্ব পালন করিবেন।

(৩) মহাপরিচালকের পদ শূন্য হইলে, বা অনুপস্থিতি, অসুস্থতা বা অন্য কোনো কারণে মহাপরিচালক তাহার দায়িত্ব পালনে অসমর্থ হইলে, শূন্য পদে নবনিযুক্ত মহাপরিচালক দায়িত্বভার গ্রহণ না করা পর্যন্ত বা মহাপরিচালক পুনরায় স্বীয় দায়িত্ব পালনে সমর্থ না হওয়া পর্যন্ত জ্যেষ্ঠতম পরিচালক অস্থায়ীভাবে মহাপরিচালকের দায়িত্ব পালন করিবেন।

( )

Now in Digital Security Act, 2018: section7:

“

7. Manpower of the Agency.

(1) The Agency shall have necessary manpower according to the organizational framework approved by the Government.

(2) The Agency may, subject to such terms and conditions as may be prescribed by rules, appoint such number of employees as may be necessary for the efficient performance of its functions. (The agency can appoint necessary number of employees to properly perform its functions. The terms of employment will be determined by rules.)

“

৭। **এজেন্সির জনবল।**—(১) সরকার কর্তৃক অনুমোদিত সাংগঠনিক কাঠামো অনুযায়ী এজেন্সির প্রয়োজনীয় জনবল থাকিবে।

(২) এজেন্সি উহার কার্যাবলি সুষ্ঠুভাবে সম্পাদনের লক্ষ্যে, বিধি দ্বারা নির্ধারিত শর্তাধীনে, প্রয়োজনীয় সংখ্যক কর্মচারী নিয়োগ করিতে পারিবে।

Here we can see all (except to select the number of employee) power is given to the executive, which may compromise the working environment and ability of an agency. Here everything is not clearly defined. In which circumventions, how the agency should react, if something gone wrong then how steps will be taken, these are not clearly defined here.
here in this section only mentioned, in which situation who will take the decision.

17 January:

Now In Digital Security Act, 2018: section8:

“

8. Power to remove or block some data-information.

(1) If any data-information related to any matter **under the jurisdiction** of the Director General, being published or propagated in digital media, creates threat to digital security, the **Director General may request the Bangladesh Telecommunications and Regulatory Commission**, hereinafter referred to as BTRC, **to remove** or, as the case may be, block the said data-information.

(2) If it appears to the **law and order enforcing force(police, RAB)** that any data- information published or propagated in digital media hampers the solidarity, financial activities, security, defense, **religious values** or **public discipline(সরক আন্দলনে অনেক পোস্ট facebook থেকে গায়েব হইয়ে যাচ্ছিল , যাতে public discipline নষ্ট না হয়)** 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**.

"

৮। **কতিপয় তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার ক্ষমতা।**—(১) মহাপরিচালকের নিজ অধিক্ষেত্রভুক্ত কোনো বিষয়ে ডিজিটাল মাধ্যমে প্রকাশিত বা প্রচারিত কোনো তথ্য-উপাত্ত ডিজিটাল নিরাপত্তার ক্ষেত্রে হুমকি সৃষ্টি করিলে তিনি উক্ত তথ্য-উপাত্ত অপসারণ বা, ক্ষেত্রমত, ব্লক করিবার জন্য বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশনকে, অতঃপর বিটিআরসি বলিয়া উল্লিখিত, অনুরোধ করিতে পারিবেন।

(২) যদি আইন-শৃঙ্খলা রক্ষাকারি বাহিনীর নিকট প্রতীয়মান হয় যে, ডিজিটাল মাধ্যমে প্রকাশিত বা প্রচারিত কোনো তথ্য-উপাত্ত দেশের বা উহার কোনো অংশের সংহতি, অর্থনৈতিক কর্মকাণ্ড, নিরাপত্তা, প্রতিরক্ষা, ধর্মীয় মূল্যবোধ বা জনশৃঙ্খলা ক্ষুণ্ন করে, বা জাতিগত বিদ্বেষ ও ঘৃণার সঞ্চার করে, তাহা হইলে আইন-শৃঙ্খলা রক্ষাকারি বাহিনী উক্ত তথ্য-উপাত্ত অপসারণ বা ব্লক করিবার জন্য, মহাপরিচালকের মাধ্যমে, বিটিআরসিকে অনুরোধ করিতে পারিবে।

(৩) উপ-ধারা (১) ও (২) এর অধীন কোনো অনুরোধ প্রাপ্ত হইলে বিটিআরসি, উক্ত বিষয়াদি সরকারকে অবহিতক্রমে, তাৎক্ষণিকভাবে উক্ত তথ্য-উপাত্ত অপসারণ বা, ক্ষেত্রমত, ব্লক করিবে।

(৪) এই ধারার উদ্দেশ্য পূরণকল্পে, প্রয়োজনীয় অন্যান্য বিষয়াদি বিধি দ্বারা নির্ধারিত হইবে।

18 January:

In **Digital Security Act, 2018: section2 subsection 1 clause (e):**

"

"computer system" means a process interconnected with one or more computers or digital devices capable of collecting, sending and storing information singly or being connected with each other; (এখানে এই সঙ্গার মাদ্ধমে digital device এর বেপারতা clear না, কয়েকটা জিনিস এর মাদ্ধেই সীমাবদ্ধ করা হয়েছে)

"

(ঙ) **"কম্পিউটার সিস্টেম"** অর্থ এক বা একাধিক কম্পিউটার বা ডিজিটাল ডিভাইস এর মধ্যে আন্তঃসংযোগকৃত প্রক্রিয়া যাহা এককভাবে বা একে অপরের সহিত সংযুক্ত থাকিয়া তথ্য-উপাত্ত গ্রহণ, প্রেরণ বা সংরক্ষণ করিতে সক্ষম;

In **Digital Security Act, 2018: section2 subsection 1 clause (j):**

"

"digital device" means any electronic, digital, magnetic, optical, or information processing device or system which performs logical, mathematical and memory functions by using electronic, digital, magnetic or optical impulse, and is connected with any digital or computer device system or computer network, and also includes all kinds of input, output, processing, accumulation, digital device software or communication facilities;

" (digital security বলতে আইন অনুযায়ী বুঝানো হচ্ছে এটা ডিজিটাল ডিভাইস অথবা ডিজিটাল সিস্টেম এর নিরাপত্তা--। জেতার মধ্যে fb,instragam, smart watch, mobile , computer পরে। কিন্তু আমদের পরার বিসয় হলঃ এসকল device use করে কোন বেক্তির অথবা রাষ্ট্রে কিছু ক্ষতি করার বাপার, miss rumor হিসেবে আস্তে পারে)

(ঞ) "ডিজিটাল ডিভাইস" অর্থ কোনো ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক, অপটিক্যাল বা তথ্য প্রক্রিয়াকরণ যন্ত্র বা সিস্টেম, যাহা ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক বা অপটিক্যাল ইমপালস ব্যবহার করিয়া যৌক্তিক, গাণিতিক এবং স্মৃতি কার্যক্রম সম্পন্ন করে, এবং কোনো ডিজিটাল বা কম্পিউটার ডিভাইস সিস্টেম বা কম্পিউটার নেটওয়ার্কের সহিত সংযুক্ত, এবং সকল ইনপুট, আউটপুট, প্রক্রিয়াকরণ, সঞ্চিতি, ডিজিটাল ডিভাইস সফটওয়্যার বা যোগাযোগ সুবিধাদিও ইহার অন্তর্ভুক্ত হইবে;

Now In Digital Security Act, 2018: section9:

"

9. Emergency Response Team.

(1) For carrying out the purposes of this Act, there shall be a **National Computer Emergency Response Team under the Agency**, for discharging duties on full time basis. (hierarchy1)

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

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

(4) The Computer Emergency Response Team shall discharge its duties in such manner as may be prescribed by **rules**, on full time basis. (executive made this role)

(5) Without prejudice to the generality **of sub-section (4),** the Computer(here parliament rules are less important than executive rules) Emergency Response Team shall discharge the following duties, namely: (subsection 4 এর rulesযেগুলা executive তৈরি করে তার বিপরিতে না যেয়ে নিচের দায়িত্ত গুল পালন করবে, rules আগে, executive বেশি powerful)(power imbalance নিয়ে q. আস্তে পারে)

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

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

or

(c) to take necessary initiatives to prevent probable and imminent cyber or digital attack;

(d) to take overall co-operational initiatives, including exchange of information with any similar type of foreign team or organization, for carrying out the purposes of this Act, with the prior approval of the Government; and

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

(6) The **Agency shall supervise** and make co-ordination among the Computer Emergency Response Teams.

"

৯। **ইমার্জেন্সি রেসপন্স টিম।**—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, সার্বক্ষণিকভাবে দায়িত্ব পালনের জন্য এজেন্সির অধীন একটি জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম থাকিবে।

(২) ধারা ১৫ এর অধীন ঘোষিত কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো, প্রয়োজনে, এজেন্সির পূর্বানুমোদন গ্রহণক্রমে, উহার নিজস্ব কম্পিউটার ইমার্জেন্সি রেসপন্স টিম গঠন করিতে পারিবে।

(৩) কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ডিজিটাল নিরাপত্তা বিষয়ে বিশেষজ্ঞ ব্যক্তি এবং প্রয়োজনে, আইন শৃঙ্খলা রক্ষাকারি বাহিনীর সদস্যদের সমন্বয়ে গঠিত হইবে।

(৪) কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, সার্বক্ষণিকভাবে দায়িত্ব পালন করিবে।

(৫) উপ-ধারা (৪) এর সামগ্রিকতাকে ক্ষুণ্ন না করিয়া, কম্পিউটার ইমার্জেন্সি রেসপন্স টিম নিম্নবর্ণিত দায়িত্ব পালন করিবে, যথা :—

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর জরুরি নিরাপত্তা নিশ্চিতকরণ;

(খ) সাইবার বা ডিজিটাল হামলা হইলে এবং সাইবার বা ডিজিটাল নিরাপত্তা বিঘ্নিত হইলে তাৎক্ষণিকভাবে উহা প্রতিকারের প্রয়োজনীয় ব্যবস্থা গ্রহণ;

(গ) সম্ভাব্য ও আসন্ন সাইবার বা ডিজিটাল হামলা প্রতিরোধের লক্ষ্যে প্রয়োজনীয় উদ্যোগ গ্রহণ;

(ঘ) এই আইনের উদ্দেশ্য পূরণকল্পে, সরকারের অনুমোদন গ্রহণক্রমে, সমধর্মী বিদেশি কোনো টিম বা প্রতিষ্ঠানের সহিত তথ্য আদান-প্রদানসহ সার্বিক সহযোগিতামূলক কার্যক্রম গ্রহণ; এবং

(ঙ) বিধি দ্বারা নির্ধারিত অন্যান্য কার্য।

(৬) এজেন্সি, কম্পিউটার ইমার্জেন্সি রেসপন্স টিমসমূহের মধ্যে সমন্বয় সাধন ও তত্ত্বাবধান করিবে।

24 January:

Now In Digital Security Act, 2018: section10: (retrospective effect)

“

10. Digital forensic lab.

(1) For carrying out the purposes of this Act, there shall be one or more **digital forensic labs under the control and supervision of the Agency.(hirearcy2)**

(2) Notwithstanding anything contained in sub-section (1), if any digital forensic lab is established under any authority or organisation of the Government before the commencement of this Act, the Agency shall, subject to fulfilment of the standard prescribed under section 11, give recognition to the forensic lab and in such case, the lab shall be deemed to have been established under this Act. (যেমনঃ ICT act2006 এও digital forensic lab বলতে একটা বিধান ছিল, যদি ICT ACT২০০৬ এর অধিনে ২০০৮ সালে একটি digital forensic lab গঠণ করে থাকে,আখন যদি অএই ল্যাব এর quality কন্ট্রোল digital security act2018 er section 11 er quality control এর মতই হই তবে তা এই আইন এর অধিনেই গঠণ বোলে ধরে নেয়া হবে।)(অতিত এর কোন জিনিস কে বর্তমানে validation দিল তাকে বলে retrospective effect)(retrospective=অতীত-সম্পর্কীয়)

(3) The **Agency shall make co-ordination** among the digital forensic labs.

(4) The establishment, use, operation and other matters of the digital forensic lab shall be prescribed by **rules. (rules=Again executive)**

“

১০। **ডিজিটাল ফরেনসিক ল্যাব।**—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, এজেন্সির নিয়ন্ত্রণ ও তত্ত্বাবধানে, এক বা একাধিক ডিজিটাল ফরেনসিক ল্যাব থাকিবে।

(২) উপ-ধারা (১) এ যাহা কিছুই থাকুক না কেন, এই আইন প্রবর্তনের পূর্বে কোনো সরকারি কর্তৃপক্ষ বা সংস্থার অধীন কোনো ডিজিটাল ফরেনসিক ল্যাব স্থাপিত হইয়া থাকিলে, ধারা ১১ এর অধীন নির্ধারিত মান অর্জন সাপেক্ষে, এজেন্সি উহাকে স্বীকৃতি প্রদান করিবে এবং সেইক্ষেত্রে উক্ত ল্যাব এই আইনের অধীন স্থাপিত হইয়াছে বলিয়া গণ্য হইবে।

(৩) এজেন্সি ডিজিটাল ফরেনসিক ল্যাবসমূহের মধ্যে সমন্বয় সাধন করিবে।

(৪) ডিজিটাল ফরেনসিক ল্যাব স্থাপন, ব্যবহার, পরিচালনা ও অন্যান্য বিষয়াদি বিধি দ্বারা নির্ধারিত হইবে।

Now In Digital Security Act, 2018: section11:

"

11. Quality control of digital forensic lab.

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

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

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

(b) ensure its physical **infrastructural facilities**;

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

(d) use quality instruments in order to maintain the technical standard of the digital test; and(এখানে technical standard নিরধারন কে করবে বলে দেয়া হই নাই)

(e) perform its functions following **scientific method** in such manners as may be **prescribed by rules**.(problem: rules are fixed but scientific methods are not fixed, if rules says to solve scientific problem in 1 day, but following scientific method a problem my or may not be solved in a specific time)

"

এ খানে Q. হতে পারেঃ digital forensic lab এর ১টা picture দিয়ে বলা হতে পারে, এই এই জিনিস গুলা ল্যাব এর মধ্যে আছে কিন্তু হতে পারে ল্যাব টা তৈরি হয়েছে ২০১২ সালে, তাহলে সেই ল্যাব টা কি এই আইন এর মধ্যে পরবে কি না? তখন section 11 এর মধ্যে quality যেগুলা আছে তার সাথে match করাতে হবে।

১১। **ডিজিটাল ফরেনসিক ল্যাব এর মান নিয়ন্ত্রণ।**—(১) এজেন্সি, বিধি দ্বারা নির্ধারিত মানদণ্ড অনুযায়ী, প্রত্যেক ডিজিটাল ফরেনসিক ল্যাব এর গুণগত মান নিশ্চিত করিবে।

(২) উপ-ধারা (১) এর অধীন নির্ধারিত গুণগত মান নিশ্চিত করিবার ক্ষেত্রে, অন্যান্য বিষয়ের মধ্যে, প্রত্যেক ডিজিটাল ফরেনসিক ল্যাব—

(ক) উপযুক্ত যোগ্যতাসম্পন্ন এবং প্রশিক্ষণপ্রাপ্ত জনবল দ্বারা উহার কার্যক্রম পরিচালনা করিবে;

(খ) উহার ভৌত অবকাঠামোগত সুযোগ সুবিধা নিশ্চিত করিবে;

(গ) উহার অধীন সংরক্ষিত তথ্যাদির নিরাপত্তা ও গোপনীয়তা বজায় রাখিবার জন্য প্রয়োজনীয় উদ্যোগ গ্রহণ করিবে;

(ঘ) ডিজিটাল পরীক্ষার কারিগরি মান বজায় রাখিবার লক্ষ্যে মানসম্পন্ন যন্ত্রপাতি ব্যবহার করিবে; এবং

(ঙ) বৈজ্ঞানিক প্রক্রিয়া অনুসরণক্রমে, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, কার্য-সম্পাদন করিবে।

Now, **Digital Security Act, 2018: section12: (Digital Security Council)**

"

12. National Digital Security Council.

(1) For carrying out the purposes of this Act, the National Digital Security Council shall consist of a Chairman and

the following **13 (thirteen)** members, namely:

(a) Chairman;

(b) Minister, State Minister or Deputy Minister of the Ministry of Post, Telecommunication and Information Technology;

(c) Minister, State Minister or Deputy Minister of the Ministry of Law, Justice and Parliamentary Affairs;

(d) Principal Secretary to the Prime Minister;

(e) Governor, Bangladesh Bank;

(f) Secretary, Posts and Telecommunication Division;

(g) Secretary, Information and Communication Technology Division;

(h) Secretary, Public Security Division;

(i) Foreign Secretary, Ministry of Foreign Affairs;

(j) Inspector General of Police, Bangladesh Police;

(k) Chairman, BTRC;

(l) Director General, Directorate General of Forces Intelligence;

(m) **Director General,** Member Secretary. l (director general কে হবে তা বলা নাই, বাকি গুলা ex-officio(জাদের আগের পদ অধিকার আছে বলে নিয়গ পাইছে))(here the director general is the director general of the agency)

(2) The Prime Minister of the Government of the People's Republic of Bangladesh shall be the Chairman of the Council.

(3) For carrying out the purposes of sub-section (1), the Council, in consultation with the Chairman, may, at any time, by notification in the official Gazette, **co-opt** any specialist as its member, on such terms and conditions as may be prescribed [such as: any specialist on recommendation of the Bangladesh Computer Samity (BCS), Bangladesh Association of Software and Information Services (BASIS), Internet Service Providers Association of Bangladesh (ISPAB), National Telecommunication Monitoring Centre (NTMC) or **1 (one) representative** of mass media on recommendation of Ministry of Information].

"

চতুর্থ অধ্যায়

ডিজিটাল নিরাপত্তা কাউন্সিল

১২। **জাতীয় ডিজিটাল নিরাপত্তা কাউন্সিল**।—(১) এই আইনের উদ্দেশ্য পূরণকল্পে, একজন চেয়ারম্যানসহ নিম্নে বর্ণিত ১৩ (তেরো) সদস্যবিশিষ্ট জাতীয় ডিজিটাল নিরাপত্তা কাউন্সিল গঠিত হইবে,—

(ক) চেয়ারম্যান;

(খ) মন্ত্রী, প্রতিমন্ত্রী বা উপমন্ত্রী ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়;

(গ) মন্ত্রী, প্রতিমন্ত্রী বা উপমন্ত্রী, আইন বিচার ও সংসদ বিষয়ক মন্ত্রণালয়;

(ঘ) প্রধানমন্ত্রীর মুখ্যসচিব;

(ঙ) গভর্নর, বাংলাদেশ ব্যাংক;

(চ) সচিব, ডাক ও টেলিযোগাযোগ বিভাগ;

(ছ) সচিব, তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ;

(জ) সচিব, জন নিরাপত্তা বিভাগ;

(ঝ) পররাষ্ট্র সচিব, পররাষ্ট্র মন্ত্রণালয়;

(ঞ) ইন্সপেক্টর জেনারেল অব পুলিশ, বাংলাদেশ পুলিশ;

(ট) চেয়ারম্যান, বিটিআরসি;

(ঠ) মহাপরিচালক, প্রতিরক্ষা গোয়েন্দা মহাপরিদপ্তর;

(ড) মহাপরিচালক - সদস্য সচিব

(২) গণপ্রজাতন্ত্রী বাংলাদেশ সরকারের প্রধানমন্ত্রী কাউন্সিলের চেয়ারম্যান হইবেন।

(৩) উপ-ধারা (১) এর উদ্দেশ্য পূরণকল্পে কাউন্সিল, চেয়ারম্যানের পরামর্শ গ্রহণক্রমে, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, নির্ধারিত মেয়াদ ও শর্তে, কোনো বিশেষজ্ঞ ব্যক্তিকে (যেমন : বাংলাদেশ কম্পিউটার সমিতি (বিসিএস), বাংলাদেশ এ্যাসোসিয়েশন অব সফ্টওয়্যার এন্ড ইনফরমেশন সার্ভিসেস (বেসিস), ইন্টারনেট সার্ভিস প্রোভাইডার্স এ্যাসোসিয়েশন অব বাংলাদেশ (আইএসপিএবি), ন্যাশনাল টেলিকমিউনিকেশন মনিটরিং সেন্টার (এনটিএমসি) বা তথ্য মন্ত্রণালয়ের সুপারিশক্রমে গণমাধ্যমের ১(এক) জন প্রতিনিধিকে ইহার সদস্য হিসাবে যে কোনো সময় কো-অপ্ট করিতে পারিবে।

25 January:

Digital Security Act, 2018: section13:

“

13. Power, etc. of the Council.—

(1) For implementation of the provisions of this Act and the rules made thereunder, the **Council shall provide necessary direction and advice to the Agency. (hierarchy3, council above agency)**

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

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

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

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

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

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

(3) The Agency shall provide necessary secretarial assistance to the Council to perform its functions.

"

১৩। **কাউন্সিলের ক্ষমতা, ইত্যাদি**।—(১) কাউন্সিল, এই আইন এবং তদধীন প্রণীত বিধির বিধান বাস্তবায়নকল্পে, এজেন্সিকে প্রয়োজনীয় নির্দেশনা ও পরামর্শ প্রদান করিবে।

(২) কাউন্সিল অন্যান্য বিষয়ের মধ্যে, বিশেষ করিয়া, নিম্নবর্ণিত কার্য-সম্পাদন করিবে, যথা :—

(ক) ডিজিটাল নিরাপত্তা হুমকির সম্মুখীন হইলে উহা প্রতিকারের জন্য প্রয়োজনীয় দিক-নির্দেশনা প্রদান;

(খ) ডিজিটাল নিরাপত্তার অবকাঠামোগত উন্নয়ন ও জনবল বৃদ্ধি এবং মানোন্নয়নে পরামর্শ প্রদান;

(গ) ডিজিটাল নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে আন্তঃপ্রাতিষ্ঠানিক নীতি নির্ধারণ;

(ঘ) আইন ও তদধীন প্রণীত বিধির যথাযথ প্রয়োগ নিশ্চিতকরণের লক্ষ্যে প্রয়োজনীয় ব্যবস্থা গ্রহণ; এবং

(ঙ) বিধি দ্বারা নির্ধারিত অন্য কোনো কার্য।

(৩) এজেন্সি কাউন্সিলকে উহার কার্য-সম্পাদনের ক্ষেত্রে প্রয়োজনীয় সাচিবিক সহায়তা প্রদান করিবে।

Digital Security Act, 2018: section14:

"

14. Meeting, etc. of the Council.—

(1) Subject to other provisions of this section, the Council may determine the procedure of its meeting.

(2) The meeting of the Council shall be held on such date, time and place as may be determined by its Chairman.

(3) The Council shall hold its meetings as and when necessary.

(4) The Chairman of the Council shall preside over all meetings of the Council.

(5) No act or proceeding of the Council shall be invalid and be called **in question** merely on the ground of any vacancy in, or **any defect in the constitution of, the Council**.

"

১৪। **কাউন্সিলের সভা, ইত্যাদি**।—(১) এই ধারার অন্যান্য বিধানাবলি সাপেক্ষে, কাউন্সিল উহার সভার কার্যপদ্ধতি নির্ধারণ করিতে পারিবে।

(২) কাউন্সিলের সভা উহার চেয়ারম্যান কর্তৃক নির্ধারিত তারিখ, সময় ও স্থানে অনুষ্ঠিত হইবে।

(৩) কাউন্সিল যতবার প্রয়োজন ততবার সভায় মিলিত হইবে।

(৪) কাউন্সিলের চেয়ারম্যান উহার সকল সভায় সভাপতিত্ব করিবেন।

(৫) কাউন্সিলের কোনো কার্য বা কার্যধারা কেবল উক্ত কাউন্সিলের কোনো সদস্য পদে শূন্যতা বা কাউন্সিল গঠনে ত্রুটি থাকিবার কারণে অবৈধ হইবে না এবং তদসম্পর্কে কোনো প্রশ্নও উত্থাপন করা যাইবে না।

31 January:

Digital Security Act, 2018: section2 subsection (1), clause (g) :

“

(g) “critical information infrastructure” means any external or virtual information **infrastructure declared by the Government** that controls, processes, circulates or preserves any information-data or electronic information and, if damaged or critically affected, may adversely affect—

(i) public safety or financial security or public health,

(ii) national security or national integrity or sovereignty;

”

(ছ) **“গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure)”** অর্থ সরকার কর্তৃক ঘোষিত এইরূপ কোনো বাহ্যিক বা ভার্চুয়াল তথ্য পরিকাঠামো যাহা কোনো তথ্য-উপাত্ত বা কোনো ইলেকট্রনিক তথ্য নিয়ন্ত্রণ, প্রক্রিয়াকরণ, সঞ্চারণ বা সংরক্ষণ করে এবং যাহা ক্ষতিগ্রস্ত বা সংকটাপন্ন হইলে—

(অ) জননিরাপত্তা বা অর্থনৈতিক নিরাপত্তা বা জনস্বাস্থ্য,

(আ) জাতীয় নিরাপত্তা বা রাষ্ট্রীয় অখণ্ডতা বা সার্বভৌমত্বের,

উপর ক্ষতিকর প্রভাব পড়িতে পারে;

Now Digital Security Act, 2018: section15:

“

15. Critical information infrastructure.—

For carrying the purposes of this Act, the Government may, by notification in the official Gazette, declare any computer system, network or information infrastructure as critical information infrastructure.

”

১৫। **গুরুত্বপূর্ণ তথ্য পরিকাঠামো।**—এই আইনের উদ্দেশ্য পূরণকল্পে, সরকার, সরকারি গেজেটে প্রজ্ঞাপন দ্বারা, কোনো কম্পিউটার সিস্টেম, নেটওয়ার্ক বা তথ্য পরিকাঠামোকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসাবে ঘোষণা করিতে পারিবে।

Now Digital Security Act, 2018: section16: (important)

“

16. Monitoring and inspection of the safety of a critical information infrastructure.—

(1) The Director General (of agency) shall, if necessary, from time to time, monitor and inspect any critical information infrastructure to ensure whether the provisions of this Act are properly complied with, and submit a report in this behalf to the Government.

(2) The critical information infrastructures declared under this Act shall, upon examination and inspection of its internal and external infrastructures, submit an inspection report to the Government every year in such manner as may be prescribed by **rules**, and communicate the subject matter of the report to the Director General.
(3) If the Director General has reason to believe that any activity of an individual regarding any matter within his jurisdiction is threatening or detrimental to any critical information infrastructure, then he may, suo moto, or upon a complaint of any other person, inquire into the matter.
(4) For carrying out the purposes of this Act, the inspection and examination of safety of any critical information infrastructure shall be conducted by a person expert in digital security.
"

১৬। গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা পরিবীক্ষণ ও পরিদর্শন।—(১) মহাপরিচালক, এই আইনের বিধানাবলি যথাযথভাবে প্রতিপালিত হইতেছে কি না তাহা নিশ্চিত করিবার জন্য প্রয়োজনে, সময় সময়, কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিবীক্ষণ ও পরিদর্শন করিবেন এবং এতদ্‌সংক্রান্ত প্রতিবেদন সরকারের নিকট দাখিল করিবেন।

(২) এই আইনের আওতায় ঘোষিত গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ, বিধি দ্বারা নির্ধারিত পদ্ধতিতে, প্রতি বৎসর উহার অভ্যন্তরীণ ও বহিঃস্থ পরিকাঠামো পরিবীক্ষণপূর্বক একটি পরিবীক্ষণ প্রতিবেদন সরকারের নিকট উপস্থাপন করিবে এবং উক্ত প্রতিবেদনের বিষয়বস্তু মহাপরিচালককে অবহিত করিবে।

(৩) মহাপরিচালকের নিকট যদি যুক্তিসঙ্গতভাবে বিশ্বাস করিবার কারণ থাকে যে, তাহার অধিক্ষেত্রভুক্ত কোনো বিষয়ে কোনো ব্যক্তির কার্যক্রম গুরুত্বপূর্ণ তথ্য পরিকাঠামোর জন্য হুমকিস্বরূপ বা ক্ষতিকর, তাহা হইলে তিনি, স্ব-প্রণোদিতভাবে বা কাহারও নিকট হইতে কোনো অভিযোগ প্রাপ্ত হইয়া, উহার অনুসন্ধান করিতে পারিবেন।

(৪) এই ধারার উদ্দেশ্য পূরণকল্পে, নিরাপত্তা পরিবীক্ষণ ও পরিদর্শন কার্যক্রম ডিজিটাল নিরাপত্তা বিষয়ে বিশেষজ্ঞ ব্যক্তি দ্বারা সম্পন্ন করিতে হইবে।

Now,
CHAPTER VI Offence and Punishment:

Digital Security Act, 2018: section17:

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

(1) If any person, **intentionally** or **knowingly**,— (এই দুটার আকটা প্রমান করলেই একটা element proved)

a) makes **illegal access** to any critical information infrastructure; or
b) by means of **illegal access**, **causes** or **tries** to **cause harm** or **damage** to it, or makes or tries to make it **inactive**, then such act of the person shall be an offence. (৬)(tries, causes)(যার ধকার অনুমতি আছে সে যদি harm damage or inactive করে তবে সেটা অপরাধ হবে না, তবে যার অনুমতি আছে সে এগুলা করে, তার অনুমতি পরে বাতিল করলে সে অপরাধি হবে)

(2) If any person— (শাস্তি)

a) commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 25 lac, or with both; and
b) commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both.

(3) If any person commits the offence referred to in sub-section (1) for the second time or repeatedly, he shall be punished with imprisonment for life, or with fine not exceeding Taka 5 (five) crore, or with both.
”

ষষ্ঠ অধ্যায়

অপরাধ ও দণ্ড

১৭। **গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে বে-আইনি প্রবেশ, ইত্যাদির দণ্ড** ।—(১) যদি কোনো ব্যক্তি ইচ্ছাকৃতভাবে বা জ্ঞাতসারে কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে —

(ক) বে-আইনি প্রবেশ করেন, বা

(খ) বে-আইনি প্রবেশের মাধ্যমে উহার ক্ষতিসাধন বা বিনষ্ট বা অকার্যকর করেন অথবা করিবার চেষ্টা করেন,

তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (১) এর—

(ক) দফা (ক) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৭(সাত) বৎসর কারাদণ্ডে, বা অনধিক ২৫ (পঁচিশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন; এবং

(খ) দফা (খ) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ১৪ (চৌদ্দ) বৎসর কারাদণ্ডে, বা অনধিক ১(এক) কোটি টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(৩) যদি কোনো ব্যক্তি উপ-ধারা (১) এ উল্লিখিত অপরাধ দ্বিতীয় বার বা পুনঃপুন সংঘটন করেন তাহা হইলে তিনি যাবজ্জীবন কারাদণ্ডে, বা অনধিক ৫(পাঁচ) কোটি টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

Q. এ ঘতনা দেয়া থাকবে। Ans আমকে সেখানে বলতে হবে যে সে অপরাধ টা করেছে কি করে নাই. যদি বলি যে সে অপরাধ টা করেছে তবে আমকে এতাও বলতে হবে যে , এই অপরাধ এর কারনে ..... এই ধারায় under e সে এই শাস্তি টা পাবে।
ত এটা করার জন্য আমকে ২টা জিনিস প্রমান করতে হবে।
element of crime→ প্রমান করতে হবে ACTUS REAS এর মাদ্ধমে ।
mental element→ প্রমান করতে হবে MENS REA এর মাদ্ধমে (Intension and knowledge)

1.ACTUS REAS(কাজ):(1st element→ access/ enters, 2nd element illegally enters, প্রথমে প্রমান করতে হবে যে প্রবেশ করেছিল এর পর প্রমান করতে হবে অবইধ প্রবেশ ছিল) আপনার কাজের সাথে সম্পর্কযুক্ত, আপ্নে কাজ তা করেছেন, এবং আপনার কাজ টার করার মাদ্ধমে element of crime(উপাদান= element of crime) (উপাদানঃ আপনার ঘরে সে প্রবেস করল [makes illegal access] -১টা উপাদান, বিনা অনুমতি তে কিছু পকেটে ঢুকাল-২য় উপাদান-চুরি করল সে) এই উপাদান গুলা যদি আমি দেখাইতে পারি (Q. এ যে ঘটনা দেয়া হয়েছে টার মধ্যে section অনুযাই সব উপাদান গুলাই আছে) তাহলে ACTUS REAS proved
2.MENS REA(mental element): Criminal offence খালি কাজ করলে হই না। criminal offence এর জন্য তাকে এটাও প্রমান করতে হবে যে টার কাজ টি করার উদ্দেস্য ছিল, এবং টার এই সম্পরকে গ্যান ছিল।(Intension and knowledge).

Digital Security Act, 2018: section18:

"

18. Illegal access to computer, digital device, computer system, etc. and punishment.—

(1) If any person intentionally—

a. makes or abets to make illegal access to any computer, computer system or computer network; or

b. makes or abets to make illegal access with intent to commit an offence, then such act of the person shall be an offence.(বাবা মা এর ফোন নিয়ে বিকাশ থেকে টাকা নেয়া)

(2) If any person— (শাস্তি)

a. commits an offence under clause (a) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 6 (six) months, or with fine not exceeding Taka 2 (two) lac, or with both;

b. commits an offence under clause (b) of sub-section (1), he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

(3) If any offence under sub-section (1) is committed to a protected computer or computer system or computer network, he shall be punished with imprisonment for a term not exceeding 3 (three) years, or with fine not exceeding Taka 10 (ten) lac, or with both.

(4) If any person commits an offence under this section for the second time or repeatedly, he shall be liable to double of the punishment provided for that offence.

"

১৮। **কম্পিউটার, ডিজিটাল ডিভাইস, কম্পিউটার সিস্টেম, ইত্যাদিতে বে-আইনি প্রবেশ ও দণ্ড।**—(১) যদি কোনো ব্যক্তি ইচ্ছাকৃতভাবে—

(ক) কোনো কম্পিউটার, কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কে বে-আইনি প্রবেশ করেন বা প্রবেশ করিতে সহায়তা করেন, বা

(খ) অপরাধ সংঘটনের উদ্দেশ্যে বে-আইনি প্রবেশ করেন বা প্রবেশ করিতে সহায়তা করেন, তাহা হইলে উক্ত ব্যক্তির অনুরূপ কার্য হইবে একটি অপরাধ।

(২) যদি কোনো ব্যক্তি উপ-ধারা (১) এর—

(ক) দফা (ক) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৬(ছয়) মাস কারাদণ্ডে, বা অনধিক ২(দুই) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন;

(খ) দফা (খ) এর অধীন কোনো অপরাধ সংঘটন করেন, তাহা হইলে তিনি অনধিক ৩(তিন) বৎসর কারাদণ্ডে, বা অনধিক ১০(দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(৩) যদি উপ-ধারা (১) এর অধীন কৃত অপরাধ কোনো সংরক্ষিত কম্পিউটার বা কম্পিউটার সিস্টেম বা কম্পিউটার নেটওয়ার্কের ক্ষেত্রে সংঘটিত হয়, তাহা হইলে তিনি অনধিক ৩(তিন) বৎসর কারাদণ্ডে, বা অনধিক ১০(দশ) লক্ষ টাকা অর্থদণ্ডে, বা উভয় দণ্ডে দণ্ডিত হইবেন।

(৪) যদি কোনো ব্যক্তি এই ধারার অধীন কোনো অপরাধ দ্বিতীয় বার বা পুনঃপুন সংঘটন করেন, তাহা হইলে মূল অপরাধের জন্য যে দণ্ড নির্ধারিত রহিয়াছে তিনি উহার দ্বিগুণ দণ্ডে দণ্ডিত হইবেন।