

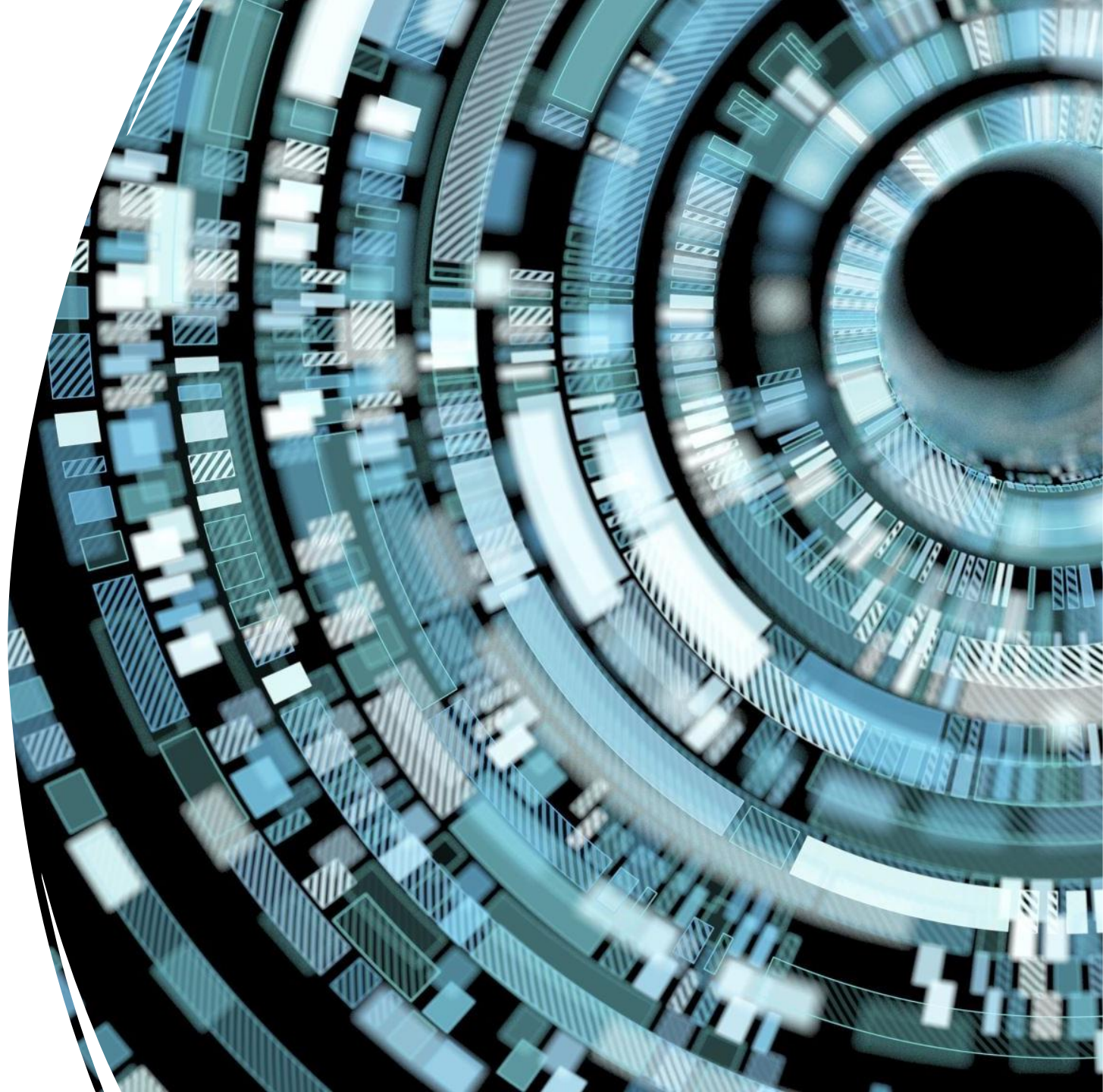
Legal Issues and Cyber Law (HUM 4747)

Md. Rafid Haque

*Department of Computer Science and Engineering
Software Engineering Programme*

ICT Act 2006 and Digital Security Act 2018: An Overview

- The two acts are the main legal frameworks for regulating information and communication technology and ensuring digital security in Bangladesh
- The objectives of this class are to:
 - Explain the objectives and scope of the two acts
 - Highlight the main provisions and offences under the two acts
 - Discuss the criticisms and challenges of the two acts



Objectives and scope of the ICT Act 2006

The ICT Act 2006 was enacted to:

- Facilitate the development of information and communication technology
- Promote e-commerce and e-governance
- Prevent and punish cybercrimes and offences
- Establish a cyber appellate tribunal

The scope of the ICT Act 2006 covers:

- Any person who commits an offence under the act within or outside Bangladesh
- Any person who causes damage to any computer, computer system or network located in Bangladesh
- Any person who receives or sends any electronic message or data from or to Bangladesh

Objectives and scope of the DSA 2018

The DSA 2018 was enacted to:

- Replace the controversial Section 57 of the ICT Act 2006
- Ensure digital security for any digital device or digital system
- Protect the sovereignty, security and integrity of the state
- Prevent and punish cyber terrorism, cybercrimes and offences
- Establish a digital security agency and a digital security council

The scope of the DSA 2018 covers:

- Any person who commits an offence under the act within or outside Bangladesh
- Any person who causes damage to any digital device, digital system or network located in Bangladesh
- Any person who receives or sends any digital message or data from or to Bangladesh

Main provisions and offences under the ICT Act 2006

- The ICT Act 2006 defines and penalizes various cybercrimes and offences, such as:
 - Hacking, damaging or destroying any computer, computer system or network
 - Altering, deleting, adding or modifying any information in a computer, computer system or network
 - Publishing, transmitting or causing to be published any obscene or indecent information in electronic form
 - Publishing, transmitting or causing to be published any information that is false, obscene, defamatory, derogatory, or prejudicial to the state or public order
 - Accessing, intercepting or using any protected system or data without authorization
 - Assisting or abetting any person in committing any offence under the act

Main provisions and offences under the ICT Act 2006

- The ICT Act 2006 also provides for the establishment of a cyber appellate tribunal, which has the power to:
 - Hear and dispose of appeals from any order or decision of a controller, adjudicating officer or agency under the act
 - Impose penalties, compensation, damages or injunctions for any contravention of the act
 - Order the confiscation or forfeiture of any computer, computer system, network or data involved in any offence under the act

Chapter Summary of ICT Act 2006

- Chapter I: Explains the **preliminary provisions** of the Act, such as the short title, extent and commencement, the definitions of various terms and concepts related to ICT, the domination of the Act over any other inconsistent law, and the inter-state application of the Act to any offence or contravention involving a computer or network located in Bangladesh.
- Chapter II: Describes the provisions of the Act regarding the **authentication, legal recognition, and use of electronic records and digital signatures** in government and its agencies, the retention of electronic records, the publication of electronic gazette, and the power of the Government to make rules for the purposes of this chapter.



Chapter Summary of ICT Act 2006

- Chapter III: Explains the concepts and rules related to the **attribution, acknowledgement, dispatch and receipt of electronic records**, and the situations when an electronic record can be regarded as being that of the originator.
- Chapter IV: Deals with **secure electronic records and digital signatures**, and the conditions and procedures for their authentication and recognition.
- Chapter V: Deals with the **controller and certifying authorities**, and their functions, powers, duties and responsibilities. It also lays down the rules and regulations for issuing, suspending and revoking digital signature certificates and licenses.



Chapter Summary of ICT Act 2006

- Chapter VI: Describes the **duties of subscribers** who use digital signature certificates issued by certifying authorities, such as applying security procedures, accepting and verifying the certificates, and preventing their disclosure to unauthorized persons.
- Chapter VII: Deals with the **penalties and confiscation** for various offences and contraventions under this Act, such as hacking, publishing fake or obscene information, misrepresentation, disclosure of confidentiality and privacy, etc.
- Chapter VIII: Deals with the **establishment of cyber tribunals** and cyber appellate tribunals, and their jurisdiction, procedure and powers for the trial and appeal of offences under this Act.
- Chapter IX: Deals with **miscellaneous** provisions, such as the protection of action in good faith, the public servants under this Act, the power of the government to make rules and regulations, and the amendment of some definitions in other Acts.





Main provisions and offences under the DSA 2018

- The DSA 2018 defines and penalizes various cyber terrorism, cybercrimes and offences, such as:
 - Committing or inciting any **act of violence or sabotage** against any person, property, infrastructure or service by using any digital device, digital system or network
 - Spreading **propaganda or campaign** against the **liberation war, the father of the nation, the national anthem or the national flag** by using any digital device, digital system or network
 - **Spreading hatred**, enmity or ill will between different groups or communities by using any digital device, digital system or network
 - Spreading information with an **intention to affect the image or reputation of the state** or to spread confusion by using any digital device, digital system or network



Main provisions and offences under the DSA 2018

- The DSA 2018 defines and penalizes various cyber terrorism, cybercrimes and offences, such as:
 - Publishing, transmitting or causing to be published any information that **hurts religious sentiments** or values by using any digital device, digital system or network
 - Publishing, transmitting or causing to be published any information that **defames any person** by using any digital device, digital system or network
 - Publishing, transmitting or causing to be published any information that **infringes the privacy** or dignity of any person by using any digital device, digital system or network
 - Publishing, transmitting or causing to be published any **information that is false, obscene, indecent, vulgar or immoral** by using any digital device, digital system or network



Main provisions and offences under the DSA 2018

- The DSA 2018 defines and penalizes various cyber terrorism, cybercrimes and offences, such as:
 - Publishing, transmitting or causing to be published any information that is related to **pornography, gambling, lottery, fraud, cheating, blackmail, extortion, harassment or intimidation** by using any digital device, digital system or network
 - Accessing, intercepting, copying, using, destroying or **damaging any protected system**, critical information infrastructure or data without authorization by using any digital device, digital system or network
 - **Assisting or abetting** any person in committing any offence under the act by using any digital device, digital system or network



Main provisions and offences under the DSA 2018

- The DSA 2018 also provides for the establishment of a digital security agency and a digital security council, which have the power to:
 - Formulate and implement policies, strategies and plans for ensuring digital security
 - Monitor, supervise and coordinate the activities of the authorities and agencies related to digital security
 - Remove or block any information published in digital media that threatens digital security
 - Investigate, search, arrest, seize or detain any person, device, system or data involved in any offence under the act

Chapter Summary of DSA 2018

- Chapter One: **Preliminary**
 - This chapter defines the key terms and concepts related to digital security, such as data storage, agency, computer system, malware, etc.
 - It also states the scope and application of the act, and its extra-judicial effect in case of offences committed inside or outside Bangladesh.
- Chapter Two: **Digital Security Agency**
 - This chapter establishes the Digital Security Agency, consisting of one director general and two directors, appointed by the government.
 - It also specifies the functions, powers, and responsibilities of the agency, and the manpower and office of the agency.

Chapter Summary of DSA 2018


- Chapter Three: **Preventive Measures**
 - This chapter empowers the director general to request the BTRC to remove or block any data-information that threatens the digital security or public order.
 - It also creates the computer emergency response team and the digital forensic lab under the agency and sets the quality standards for the lab.
- Chapter Four: **Digital Security Council**
 - This chapter forms the National Digital Security Council, chaired by the prime minister, and consisting of 13 members from various ministries and institutions.
 - It also outlines the powers and functions of the council, such as providing directives and advice to the agency, ensuring the security of critical information infrastructure, and enacting inter-institutional policies.
 - It also determines the meeting procedures and secretarial support for the council.

Chapter Summary of DSA 2018

- Chapter Five: **Critical Information Infrastructure**
 - This chapter empowers the government to declare any computer system, network, or information infrastructure as critical information infrastructure, which is vital for national security, public safety, or public health.
 - It also authorizes the director general to visit and inspect the security of critical information infrastructure, and to investigate any threat or harm to it.
- Chapter Six: **Crime and Punishment**
 - This chapter defines various offences and punishments related to digital security, such as illegal entrance, damage, forgery, fraud, identity theft, propaganda, defamation, e-transaction, etc.
 - It also provides for compensation, confiscation, and delegation of power in case of offences.

Chapter Summary of DSA 2018

- Chapter Seven: **Investigation of Offence and Trial**
 - This chapter specifies the investigation officer, the time limit of investigation, the power of investigation officer, the secrecy of information, the cognizance of offence, the adjudication of offence, and the appeal process.
 - It also states the application of the code of criminal procedure, the opinion of expert, and the classification of offences.
- Chapter Eight: **Regional and International Assistance**
 - This chapter states that the provisions of the Crime Related Interpersonal Assistance Act, 2012 will be applicable in case of regional or international assistance for investigation or trial of offences under this act.
- Chapter Nine: **Miscellaneous**
 - This chapter contains some miscellaneous provisions, such as the delegation of power, the activities done in good faith, the power to make rules, and the power to remove difficulties.



The criticisms and challenges of the ICT Act 2006 & DSA 2018

- The act has a **vague and broad definition** of the term “cybercrime”, “digital security”, “defamation”, “sedition”, and “hurting religious sentiments” that can be interpreted arbitrarily and subjectively
- The act **grants excessive and unchecked powers** to the authorities to arrest, search, seize, and block any information or device without a warrant or judicial oversight
- The act imposes harsh and disproportionate penalties, such as imprisonment for up to **14 years** and fines up to **10 million taka**, for non-violent and minor offences
- The act creates a chilling effect on the **freedom of expression** and the press, as journalists, activists, bloggers, and citizens face harassment, intimidation, and censorship for expressing their opinions or reporting on sensitive issues

A case study of the ICT Act 2006

- In 2017, a journalist named **Abdul Latif Morol** was arrested and charged under Section 57 of the ICT Act 2006 for posting a **satirical comment on Facebook about a dead goat given to him by a local politician**.
- He was accused of publishing false, obscene, or **defamatory** information that could hurt the image or reputation of the politician.
- He was **denied bail by the lower court** and had to spend more than two months in jail.
- He appealed to the High Court Division of the **Supreme Court** of Bangladesh, which **granted him bail** and observed that his comment was not defamatory, but rather humorous and sarcastic.
- The High Court also criticized the **misuse and abuse of Section 57** of the ICT Act 2006 and urged the government to amend or repeal it.



A case study of the Digital Security Act 2018

- In 2020, a cartoonist named **Ahmed Kabir Kishore** was arrested and charged under several sections of the Digital Security Act 2018 for **drawing cartoons** that criticized the government's response to the Covid-19 pandemic.
- He was accused of spreading false, distorted, or misleading information that could create panic, confusion, or disorder among the public or damage the image of the state or a person.
- He was denied bail by the lower court and had to spend more than **10 months in jail**, during which he suffered from **torture** and ill-treatment.
- He appealed to the High Court Division of the **Supreme Court** of Bangladesh, which granted him **bail** and observed that his cartoons were an **exercise of his freedom of expression** and artistic creativity.
- The High Court also expressed concern over the arbitrary and excessive use of the Digital Security Act 2018 and called for its review and reform.





Thanks