➢ **What is cyber-crime?**

You often hear the term 'cybercrime' bandied about these days, as it's a bigger risk now than ever before due to the sheer number of connected people and devices. But what is it exactly? In a nutshell, it is simply a crime that has some kind of computer or cyber aspect to it.

Common types of cybercrime include **hacking**, **online scams** and **fraud**, **identity theft**, **attacks on computer systems and illegal or prohibited online content**. The effect of cybercrime can be extremely upsetting for victims, and not necessarily just for financial reasons.

Cyber Law in Bangladesh is an interesting yet evolving sector of Law. But what is it that contemplates the true meaning of Cyber Law? Well, the term Cyber Law derived from its generic term called Cybernetics, which means that this sector of law tend to resolves issues, and legal consequences that are raised in the Internet.

And what makes Cyber Law in Bangladesh even a legal factor, honestly speaking, everything does. With time and generation the virtual world is becoming more familiar than reality, however, even than check and balances for the crimes committed in the virtual world can only be resolved through a practical commission of natural judicial process. Which in turn needs assistance from Cyber Law.

Currently, the realm under which cyber law resides in Bangladesh is the ICT Act 2006 as amended in 2013. Funny but true the Act does not provide any definition as to what is Cyber Law.

One of the most important provisions, probably most controversial as well, is the section 57 of the ICT Act. Basically, the section heavily condemned several online crimes such as defamation, pornography, illicit propaganda against the government or religious belief into one section.

1. Now this section is very controversial due to its vague nature, which is subject to several different interpretations, hence it's not specific as to what may constitute an offense under the section.

2. Recently, amended version of the section in 2013, increased the penalty for violation of the provision from maximum imprisonment of 10 years to 14 years and a minimum of 7 years. Now that's a heavy penalty imposed for the lenient version of the crime.

In the mist of all these, as of now the section is the ultimate resort for people who are being defamed or aggrieved online. The Act further considers other technical crimes such as hacking and spamming. Nevertheless, its always better to be cautious than ignorant, and irrespective of all the legal jargons, it is wise to refrain ourselves from commenting or posting materials that may harm others both ethically and from legal point of view. Because You never know you might easily be an offender under Cyber Law.

Out of all legal remedies offered by the state, Writ is a crucial form of legal remedies against the infringement of the administrative actions which is getting much more popular upon several successful applications as a remedy in the context of the adverse activities of the state bodies. If effective measures are taken and brought to the court maintaining the proper procedure, Writ Petition in Bangladesh can be demonstrated as an effective remedy for the public as a special modification in the existing legal and administrative system of Bangladesh.

Information technology law (also called "cyberlaw") concerns the law of information technology, including computing and the internet. It is related to legal informatics, and governs the digital dissemination of both (digitalized) information and software, information security and electronic commerce. aspects and it has been described as "paper laws" for a "paperless environment". It raises specific issues of intellectual property in computing and online, contract law, privacy, freedom of expression, and jurisdiction.

Bangladesh is planning stringent measures to fight cyber crime amid the rapid expansion of the information and communications technology and telecommunications networks in the South Asian country. Bangladesh's ICT industry has been expanding exponentially and is making its presence strongly felt both in the public and private sectors. More than five million personal computers are now in use in the country with three million internet users, by industry estimates. "We have taken steps to facilitate fair and secured use of information technology as the country lacks a complete law to deal with cyber crime," says MM Neazuddin, Joint Secretary to the Science and ICT Ministry. Neazuddin said that the government, which has pledged a "Digital Bangladesh" by the year 2021, had approved in principle to amend previous legislation calling for jail terms and heavy financial penalties to tackle new forms of crime. The proposed law has suggested provisions for a maximum 10 years in jail and taka 10 million (US$150, 000) in fines for hacking into computer networks and putting false and libellous information or indecent material online. For the speedy and effective prosecution of the offences, the government will consult with the Supreme Court to set up one or more Cyber Tribunals.

The Penal code of Bangladesh contains very few provision regarding cyber squatting. But in case of cyber crime like Hacking, Internet time thefts, Email bombing- there is nothing contained in our penal code. So it can be said that it is not possible for our government to control cyber crime by using some provision of the penal code. To controlled cyber crime it is necessary to enact special law which only deals with cyber related matters.

The Government of Bangladesh passed Information Technology Act on 2006. This is the most recent statute enacted by the government of Bangladesh with a view to consolidate Computer related matters and also prosecute computer and computer network related Offence. This statute contains several provisions regarding damage to computer and computer system.

Cybercrime dictates that prohibits attacks or unauthorized access to computers and computer systems. According to Section 66 of the ICT Act provides Punishment for tampering with computer source documents. Section 66 says whoever intentionally destroys or alters or intentionally or knowingly causes any other person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine which may extend to Taka two lakhs, or with both.

Section 67 Hacking with computer system. Whoever, with the intent to cause or knowing that he is likely to cause wrongful loss or damages to the public or any other person, does any act and thereby destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits the offence of "hacking".

Section 68 of the ICT Act provides punishments for the hackers. Section 68 says that whoever commit hacking shall be punished with imprisonment for a term which may extend to three years or with fine which may extend to taka two laks or with both. But the problem of this act is this act deals with so many things. The act is made to cover all the information technology related matters. But it is not possible to cover all the things by implementing just only one act. In order to control cyber crime we need to have one specific cyber law in our country.

Digital Security Act (DSA)

The Digital Security Act (DSA) was enacted in 2018 to provide cyber security to citizens, but its wide scope and vague provisions are being exploited for more nefarious purposes.

Human rights defenders have repeatedly highlighted that the act can be used as a weapon to muzzle contrarian voices from exercising their freedom of expression, particularly the press, but this is only the tip of the iceberg of problems that it poses. The act can be abused to harass anybody from any profession, not just journalists.

The most dangerous aspect of the DSA is the wide range of offences it considers cognizable and non-bailable. Such offences allow police to conduct an investigation and carry out an arrest without an order of the court or warrant, and the accused has no choice but to languish in jail until he is tried.

Even if the case is eventually dismissed, the damage has already been done.

THE TARGETS OF DIGITAL REPRESSION

In the past three years, more than 1,500 cases have been filed under the DSA. These cases are under the purview of eight cyber crimes tribunals. The author has gathered information about 754 cases filed between January 1, 2020, and October 31, 2021, as part of a project funded by the National Endowment of Democracy for the Centre for Governance Studies in Bangladesh, a project for which the author is the principal investigator.[1] These data were collected from government-approved print and electronic media; the accused or their family and friends; the lawyers of the accused; and police stations and other concerned departments.

Digital Security Act-2018

Digital Security Act-2018

The Digital Security Act was passed by the Bangladesh parliament in 2018 after 5 controversial sections of the Information and Communication Technology Act/ ICT Act were eliminated, they were Section 54, Section 55, Section 56, Section 57, and Section 66. Since the DSA Act-2018 came into force, journalists, social and human activists, educators, members of civil society, diplomats, and various international organizations strongly objected to nine sections of the law, which they described as detrimental to freedom of speech; these Sections are 8, 21, 25, 28, 29, 31, 32, 43 and 53.

Since the law came into effect, a total of 757 cases have been registered under the Digital Security Act 2018 until the end of 2019. Of these, 126 cases were filed in 2018, and 631 cases were filed in 2019. About 1649 people have been accused and more than 733 accused have been arrested in these cases. People from almost all walks of life, including newspaper editors, journalists, educators, poets, publishers, politicians, activists, and lawyers have been charged under the DSA.