Chapter II

CONCEPT OF DIGITAL DEFAMATION

We know that as the Internet grows, there will be more and more lawsuits involving libel and defamation, Says attorney David H.[1]

The same technology that gives you the power to share your opinion with thousands of people also qualifies you to be a defendant in a lawsuit. Says Professor Nicholas Johnson, Iowa University School of law.[2]

> Cyber defamation need not necessarily be directed against an individual victim, but it could be harmful to the whole society. It could be directed against an individual, but the criminal act is potentially capable of harming a large number of persons and that is the principal object behind punishing it.[3]

Lord Bingham of Cornhill said that, the law of defamation in the context of the internet would require almost every concept and the rule in the field to be considered in the light of this unique medium of instant world-wide communication.[4]

## 2.1 DEFAMATION

Generally, defamation consider as false and unprivileged speech or statement of fact that is harmful to someone's reputation, or prestige and published "with fault," meaning as a result of negligence or malice. State laws often define defamation in specific ways. Libel is a written defamation; slander is a spoken defamation.

## 2.2 DIGITAL DEFAMATION

Digital defamation considers as false and unprivileged speech or statement of fact that is harmful to someone's reputation, or prestige and published "with fault," meaning as a result of negligence or malice through digital way (as like social site or any digital print media). State laws often define digital defamation in specific ways. Libel is a digital written defamation; slander is a spoken defamation through online.

There are two major types of defamation: libel, or scripted or written defamation, and slander, or unwritten defamation. When a theoretically insulting statement is made online or via social media -- such as via Facebook or LinkedIn that involves the written (or "posted") word, and so it is deemed libel.



[1] Rindos V Hardwick, 1993 ALR
[2] Suarez Corporation Industries V Brock Meeks, 1994, ALR
[3] http://www.lawyersclubindia.com/articles/print_this_page.asp?article_id=644
[4] Collins, M., (2005) *The Law of Defamation and the Internet,* Oxford University Press.

## 2.3 PROBLEM OF ONLINE DAFIMATION

The internet and social media are absolutely a great invention for people and society in general, but they are also an individually effective breeding ground for potentially defamatory statements.

Lots people have learned (to their dismay) that the cyberspace lets people to express their mind word practically too easily. The internet is chock-full of fascinating web sites where someone could on purpose or accidentally leave a potentially defamatory comment or post.

Just a few of these locations are:

- Firstly, letters to the editor of local newspapers
- Secondly, public comments on media (i.e., newspaper or magazine) web sites
- Thirdly, blogs and comments to blog postings
- Fourthly, social media like Facebook, LinkedIn, and Twitter, and
- At last chat rooms or list servers.

While some web sites show posts for inflammatory or illegal content of their site, the screening methods are not geared to examine every post for defamatory content, and so many defamatory postings end up online media.

## 2.4 TYPRS OF DEFAMATION

Defamation can be bifurcated into two categories and these are –

- **Libel** – A statement that is defamatory or insulting and is published in a written form.
- **Slander** – A defamatory or insulting statement spoken that means a verbal form of defamation.

Thus, the fundamental distinction between both the types is the medium in which they are expressed that is, one is expressed in a written form while the other in oral form.

Though, this article will spotlight solely on libel because the Internet is considered a permanent method, and as such, most online subject matter—even videos—falls into the libel category.

While defamation laws vary from state to state, the threshold for determining if a statement is defamation is generally the same. For a statement to qualify as defamation, it must be:

- **Published:** This just means that the declaration or speech was made public, not that it was printed in a book or print media. But Something shared on the Internet is considered "published."

- **False:** If a statement is not false, it cannot reasonably hurt your reputation. Consequently, views like That was the worst hamburger I have ever eaten. Usually do not count as defamation because it is difficult to prove these statements are false. After all, how can anyone know or judge the quality of all the hamburgers someone else has consumed? However, if somebody stated, do not go to this business: They stole $500 from me! and you can prove you have never done business with that person, then that would be defamation. It was a lie they knew to be false, spread with the intent to damage your reputation.

- **Injurious:** The point of defamation law is to pay compensation people for hurts to their reputations. Hence, you need to show how a false statement has damaged your status. For example, it cost you your job, hurt your business, or ruined your relationships. Because of this, people who had bad reputations to begin with usually do not get much benefit from a defamation lawsuit.

- **Unprivileged:** In specific situations, people are protected (privileged) from being sued for defamation. For example, when a person is appearing in court or when someone is trying to inform others about something unsafe.

## 2.5 SHOULD YOU FILE A LAWSUIT ON THE DIGITAL DEFAMATION **

When it comes to online defamation, most people's first thought is should I hire a lawyer? The answer is it depends on your situation."

Filing a defamation suit can be a smart strategy in certain situations. Even then, however, it is rarely enough on its own. You may win legal respite, but that will not necessarily stop the defamatory information from spreading across the Internet.

When deciding whether to take the legal route, you need to consider a number of factors, including the strength of your reputation prior to the attack (a well-established online image can serve as a buffer against defamatory attacks) and how much time and money you have available to devote to the case.

The most important thing to know is that filing a lawsuit can trigger the Streisand effect, which is when an attempt to cover up sensitive information ends up amplifying it instead, especially if the information in question is scandalous or otherwise gossip worthy. A reporter coined this term in 2005 after Barabara Streisand went to court to make a photographer remove a photo of her home from his website. Before Streisand

filed the lawsuit, the photo had only been downloaded a handful of times. As a result of the publicity surrounding the case, the image gained nearly half a million views.[5]

> The same thing can happen when you file a defamation lawsuit. Because of the salacious nature of defamatory remarks, news about these kinds of cases tends to spread quickly. This means that even more people will see the negative remarks you are trying to remove. Thus, by trying to force someone to remove a defamatory remark, you might end up making the situation worse and causing more damage to your reputation. Another thing to consider before deciding to hire a lawyer is that lawsuits can be lengthy and expensive, even if you have a slam-dunk case. This is because it can be difficult to identify the person defaming you, as the famous Liskula Cohen case demonstrated. And it can be even harder to prove that someone has engaged in defamation.[6]

## 2.6 WHAT STATES LAW APPLIES? WHERE CAN YOU SUE FOR DIGITAL DEFAMATION?

This is a difficult issue that hangs on what state you live in, what state the alleged defamer lives in, and the contacts that the defamer has had with your state, if any. If you think that you have been defamed by computer, you should contact a qualified attorney as soon as possible to talk about your legal options and the best course of action.

## 2.7 DAMAGES FOR DEFAMATION **

In most states, the plaintiff must also prove that the defamatory statement caused him or her actual damage. Actual damages include such things as the loss of a job because of the defamatory statement but can also include mental anguish or suffering associated with the defamation. Some jurisdictions also recognize "per se" defamation, where damage is presumed if the defamatory statement relates to one of the following subjects:

- Impugns a person's professional character or standing.
- States or implies that an unmarried person is unchaste (e.g., is sexually active).
- States or implies that a person is infected with a sexually transmitted disease; or
- States or implies that the person has committed a crime of moral turpitude (e.g., theft or fraud).

## 2.7 PARALLEL LAGAL CLAIMS BASED ON ALLEGEDLY FALSE STATEMENT **

It is common for defamation plaintiffs to assert not only a claim for defamation, but also claims for infliction of emotional distress, interference with business relationships, etc.,



[5] Mike Masnick of Techdirt coined the term in 2005
in relation to a holiday resort issuing a takedown notice to urinal.net (a site dedicated to photographs of urinals) overuse of the resort's name.
[6] Cohen v. Google Inc. and Blogger.com (New York Sup. Ct., 2009)

arising out of the same allegedly false statements. These parallel claims will ordinarily be subject to the same limitations, privileges, and defenses as the main defamation claim. For more information, see our section on Other Falsity-Based Legal Claims.

## Chapter III

## DIGITAL DEFAMATION IN BANGLADESH

### 3.1 INTRODUCTION

Crimes committed due to misuse of social networking sites are becoming a serious matter in Bangladesh as well as whole over the world. Study the key objective of this paper is to examine how social networking websites are being misused in committing crimes especially defamation on online environment in Bangladesh and to analyze the legal frameworks and the attitudes of judiciaries of these jurisdictions on the present matter. It also attempts to identify the certain issues and challenges. Social Networking Sites particularly Twitter & Facebook are leading to various offences especially offensive and defamatory speech in those platforms. Although legal instruments recognize such activities as offences, the controlling of those is being affected due to existence of certain substantive as well as procedural lacuna in laws and ineffective enforcements mechanisms. The scope of crimes committed in cyber space due to misuse of social networking sites is wide, but the ambit of this paper is limited to offensive statements especially cyber defamation. It is not going to distinguish defamation committed online environment under civil or criminal laws rather to analyze defamation committed in Bangladesh through Facebook & Twitter.

### 3.2 CYBER CRIME IN BANGLADESH

Generally, cyber-crime is a crime committed in cyber space or on online environment. It is defined as an unlawful act wherein the computer is either a tool or a target or both.[7] Computer using as a tool or medium means computer is being used to commit another crime prescribed in criminal laws e.g., inducing to commit any crime through posting or sharing statement in any blogs, Facebook, or Twitter. And computer is used as a target means damaging computer through internet e.g. posting malware to access without authorization known as hacking.



[7] The Penal Code. s. 500.

Cybercrime is a worldwide problem now. As it is known that there is no universal definition of crime. Generally, a crime is an anti-social act for which punishment is available. When a crime is committed in cyber space or online environment, it is defined as a cyber-crime; hence, a cyber-crime is constituted with all elements of particular offences, plus admissibility of cyber space. It may be argued that cyber space is not real, so doing antisocial act will not be treated as crime. If any anti-social activity committed in real world is an offence, such anti-social action committed online in any platform or format should be considered as an offence as activities bear similar effects in cyber space as bears in real space.

There are diverse of crimes may be committed on online social networking platforms. For examples, copyright violation or unauthorized data sharing, piracy, harassment, cyber pornography, online fraud, identity theft, provocation to commit crime etc. can be committed in or by using Facebook. Moreover, users may contain offensive contents including cyber threat or extortion to injure defamatory statement and hate speech etc. in his or her Facebook or Twitter plot.

In a case, a person posted a defamatory and threatening statement against Prime Minister of Bangladesh in his Facebook profile. He was charged under section 57 of the Information and Communication Technology Act 2006 for committing cyber defamation. He was tried expartee as he did not serve his defense. On January 4, 2012, the High Court Division sentenced him to six months in jail for disregarding a court summons and contempt of court rule in connection with derogatory comments on the prime minister on Facebook.[8]

It was not possible to implement such punishment as alleged offender lives outside of the country, although the court directed the foreign secretary to take steps to bring accused. In another case where on April 23, 2012 a complaint was filed accusing Hafizur Rahman Rana for issuing death threat to Prime Minister on his Facebook wall. On September 20, 2012, the charges against accused were framed and decided to try him in absentia as he did not appear in the court. On 27th June 2013, Dhaka Metropolitan Sessions Judge sentenced the accused in his absence to five years under section 57 of ICTA 2006 for publishing fake, obscene or defamatory information in electronic form, and to two years under section 506 of the Penal Code for criminal intimidation.[9] This is a historic verdict as it is the first ever judgment under the ICTA 2006. On 8 October 2013 another allegation was made against Mr. Wahiduzzaman for posting defamatory statement in Facebook against the son and sister of Prime Minister made on August 22 in the same year. He was arrested and is still in jail, and the charge against him was framed under ICTA for making defamatory statement.[10] In all of the stated cases brought before the



[8] Death Threat to PM on Facebook, Former BUET teacher gets 7yrs in jail. (2013, June 28). New Age (Online Ed.). Retrieved from http://www.newagebd.com/detail.php?date=2013-06-28&nid =54778#. UyCL5IXXiOp (2014, March 13).

[9] Ibid

[10] The report was published on 10th February 2014 in bangle in http://tazakhobor.com

court under ICTA 2006, defamatory comments were made against political figures of ruling party.

From these incidents, there is a chance of realisation that law enforcement agencies might be influenced as political bias could be involved in the proceedings. In early 2013, some social networking sites users started to use defamatory statements on social media against the religion of Islam. The government formed a committee to track such users. Four anti-Islamist bloggers and Facebook users have been arrested in different areas in the capital on suspicion of making derogatory comments about Islam. On 09-09-2013, the Dhaka Metropolitan Sessions Judge's Court has charged four in two cases under sections 57(1) & 57(2) of the ICTA for inflammatory writeups and hurting religious sentiments in online platforms (for hurting religious sentiments).[11]However, the proceedings of the two cases were challenged in the High Court Division, and on February 16, 2014 the court ruled a stay of proceedings for three months.[12]This is the first time any accused has been charged under the ICTA after it was amended. If their guilt is proved, they could be awarded between seven and fourteen years in prison or to fine upto BDT 10 million or both, under the amended provisions.

In Bangladesh, particularly young women are more likely than men to face severe online abuse that is sexualized and violent. In spite of weak institutional protection, women often make formal report of harassment, abuse, and violence originated from online spaces. According to a study, 73 percent of women internet users have reported cybercrime (Zaman, Gansheimer, Rolim, & Mridha, 2017). As of December, 2017 the government's Information and Communication Technology Division's Cyber Help Desk has received more than 17,000 complaints, 70 percent of complainants were women.

### 3.3 LEGAL REGIME IN BANGLADESH

For the purpose of controlling cyber-crimes including defamation committed in cyber environment, the Information and Communication Technology Act 2006 (hereinafter called ICTA) was enacted in Bangladesh. Section 57 of the present Act criminalizes any deliberate publishing or transmitting or causing to publish or transmit on the website or in electronic form any material which is fake and obscene or its effect is such as to tend to deprave and corrupt 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 to deteriorate law and order, prejudice the image of the State or person or causes to hurt or may hurt religious belief or instigate against any person or organization, then this activity of his will be regarded as an offence, and shall be punishable with imprisonment for a term which may extend a minimum of 7 years and a maximum of 14 years or with a fine which may extend to BDT 1 crore (10 millions) or with both.[13]Moreover, the Penal Code 1860, a general criminal law, also



[11] Retrieved from http://www.globaltimes.cn/content/809498.shtml#.Ur1i4VGczIU(2013, November 20 )

[12] The news of this stay proceedings was published on 16th February 2014 in bangle in http://www.banglanews24.com

[13] The original section 57 prescribed maximum imprisonment of 10 years and of fine of 1 crore taka. By virtue of the Information and Communication Technology (Amendment) Act 2013, penalties for

describes defamation as an offence. According to section 499 of the said Code, subject to certain exceptions mentioned in the present section making or publishing any imputation concerning any person, intending to harm or knowing or having reason to believe that such imputation will harm the reputation of such person, by words either spoken or intended to be read or by signs or by visible representations is a punishable offence. Additionally, in the legal system of Bangladesh it is also open for the defamed person to acts under tort law, and claim damages for making and publishing any defamatory statement.

### 3.4 LAW ENFORCEMENT MECHANISMS IN BANGLADESH FOR ONLINE DEFAMATION

No matter how good a law is, if there is no enforcement mechanism, it is dead letter. The laws of both jurisdictions tried to set up various enforcement mechanisms to fill up these relevant gaps. The ICTA authorizes the police to arrest without warrant for the purpose of effective enforcement by way of inserting offences as cognizable. In 2013, the ICTA established a first track process in the form of cyber tribunal which acts under its parent law dealing with cyber-crimes in Bangladesh. Less political will is one of the dilemmas in the enforcement of any laws shown in the attitudes of legislature as special tribunal has been established after long time as the ICTA was passed in 2006. Law enforcement agencies comparatively have little expertise on cyber issues.

The ICTA made electronic data produced by computer, for example, e-mails as admissible evidence,[14] conflicting with the country's Evidence Act 1872 which does not recognize the same as evidence. By contrast, Malaysia resolves it by inserting sections 90A, 90B & 90C in Evidence Act 1950.It may be argued that Evidence Act of Bangladesh does not prohibit e-data, how can it be said that it is not recognizing the same. Interpretation clause of Evidence Act defines 'document' as "any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter". [15]Whether online platform is a substance or not is an unsettled issue.

### 3.5 JUDICIAL VIEWS IN BANGLADESH

In 2006, an English court in Keith-Smith v Williams confirmed that the existing libel law applies on net.[16] Similarly, the attitudes of judiciaries of Bangladesh is also positive as the crimes committed on online platforms specifically Facebook and Twitter are being enforced in the court of law. The number of Facebook and Twitter users in Bangladesh experiences might be equal as in both Facebooking and twitting cases are being brought before the court of laws, whereas almost all cases regarding cyber-crimes including cyber defamation and religious insult committed due to misuse of Facebook were come before



cybercrimes were increased by setting a minimum of seven years imprisonment and a maximum of 14 years or a fine of Tk 1 crore or both

[14] The ICTA. s. 13

[15] The Evidence Act 1872. s. 3.

[16] Retrieved from http://www.theguardian.com/media/2006/mar/23/digitalmedia.law (2014, January 2)

the judiciary of Bangladesh. Bangladesh is common law countries and adopted tort law from English laws. By virtue of sections 3 & 5 of Civil Law Act 1956.

Though there is no binding authority, the courts of Bangladesh also follow English rule as persuasive authority. From the judicial cases, Bangladesh courts experienced all the cases because of improper use of Facebook invoked as criminal offences which doesn't mean there is no application of tort law rather means there is very rear tort application. Defamation committed in Twitter and Facebook is well established in Bangladesh by judicial precedents, that is to say, some cases have already been decided by the High Courts and some of under trail. Some of cases brought before higher judiciary in Bangladesh who makes binding precedent in Bangladesh scenario. In Bangladesh, the trend to come before the court on said issues are started before but most all cases are pending before lower courts and very few cases decided by trial court. If these cases will go to higher court by way of appeal or by any lawful application, it is thought that issues will be considered in the same line as it was thought by the other country judiciary. In order to establish a defamation case in the court of law, the claimant has to prove that the defendant made a false and defamatory statement concerning the plaintiff, which is injurious to him, and published it negligently which was unprivileged.[17] In the case of Ayoba bin Samad v TS Sambanthamurthi, Mohamed Dzaiddin J. held that in defamation cases, the burden lies on the plaintiff to prove that the statements or words bearing a defamatory meaning; the statements or words referring to the Plaintiff; and the statements or words which formed the subject matter of the action had been published. [18]If the statement is true, the person against whom statement was published does not have grounds to sue, even if it damaged his or her reputation.

Therefore, it can be stated that like a real-world defamatory claim, same legal requirements should be taken into consideration by the courts to decide a defamation matter on any online platform including Facebook and Twitter.

Bangladesh legislated an 'ICT Act' in 2006 (amended in 2013) to combat cybercrime and online harassments. However, the provisions of this Act are quite insufficient to undertake legal measures appropriately as it does not address gender-based violence online in a clear and effective manner. Similarly, the 'Telecommunication Act 2001' does not address the gender-based violence that occurs via the use of telecom networks or the internet. The Pornography Control Act is not properly used to combat cyber violence because of the institutional corruption and powerful allies with the ruling politics. The influential remains safe always if the victims are poor. Also, Bangladesh has formed a 'Cybercrime Tribunal' that addresses cyber violence. However, according to most accounts, around 90 percent of the instances of online violence are not reported by the victims. Information received under Right to Information (RTI) Act reveals - "from 28.07.2013 to 10.02.2016, the Cybercrime Tribunal received 520 cases of which 328



[17] iRetrieved from http://injury.findlaw.com/torts-and-personal-injuries/elements-of-libel-andslander.html#sthash.fTwUgMF0.dpuf (2013, November 11)
[18] x[1989] 1 MLJ 315; [1989] 1 CLJ 152; [1989] 1 CLJ (Rep) 321;

cases were dropped." News media in Bangladesh are mostly unable to notice the angel of gender violence in cybercrime.

Bangladesh police have opened a cyber wing to deal with the increasing number of cyber threats and it is responsible for monitoring cybercrimes and tracking the criminals. But gender-based violence online is not covered as a specific action. Also, Bangladesh Telecommunication Regulatory Commission (BTRC) is working to regulate and monitor cybercrime. This commission blocks inappropriate websites, blogs, and Facebook accounts. On the other hand, there is concern that sometimes the overreach of legal tools related to the safety of women in cyberspace help the enforcing agencies to create restriction of freedom of expression. For instance, some victim of cyber violence take legal action under section 57 of ICT Act which also criminalizes the posting online of inflammatory or derogatory information against the state or individuals, thus stifles freedom of speech. Though the percentage of women among people who invoked section 57 of ICT act is very low (Zaman, Gansheimer, Rolim, & Mridha, 2017). A Right to Information application received a response that, out of 520 cases filed under the law over three years, 90 cases were filed by women between March 2013 to February 2016.

## Chapter IV

## REGULATION OF BNGLADESH AND DIGITAL DEFAMATION: COMPARATIVE STUDY

### 4.1 LEGAL RESPONSE TO CYBER CRIME IN BANGLADESH

In order to facilitate e-commerce and encourage the growth of information technology, the ICT Act, 2006 was enacted making provisions with a maximum punishment of 10 years imprisonment or fine up to taka 10 million or with both. However, recently our Parliament amended the ICT Act 2006, raising penalties for cybercrimes setting a minimum of 7 years imprisonment and a maximum of 14 years or a fine of Tk. 1 core

or both. The bill made offences under sections 54, 56, 57 and 61 of the ICT Act, 2006 cognizable and non-bail able, empowering law enforcers to arrest anyone accused of violating the law without a warrant, by invoking section 54 of the Code of Criminal Procedure.

All such offences were non-cognizable in the ICT Act, 2006. However, all concerned apprehend of the misuse of the power by the police. The ICT Act, 2006 as amended in 2013 is obviously a brilliant achievement of Bangladesh in the field of cyber law. Critics point out that still there remain certain specific limitations of the said Act as under.

(i) The Act remains silent about various intellectual property rights like copy right, trademark and patent right of e-information and data.
(ii) The enactment has a major effect on e-commerce and m-commerce in Bangladesh. But it keeps itself mum as to electronic payment of any transaction.
(iii) The legislation was initially supposed to be applied to crimes committed all over the world; but nobody knows how this can be achieved in practice.
(iv) Spamming has become a peril in the west as such they have made anti spamming provisions in cyber law. However, there is no anti spamming provision in our Act.
(v) Domain name is the major issue which relates to the internet world thoroughly. But the ICT Act, 2006 does not define 'domain name' and the rights and liabilities relating to this.
(vi) The Act does not address any crime committed through using mobile phones.
(vii) This law made e-mails as evidence, conflicting with the country's Evidence Act that does not recognize as e-mails as evidence. We hope our government would take proper initiative to get rid of the problems for ensuring a cyber-crime free peaceful society.

## 4.2 NECESSARY LEGISLATIONS IN BANGLADESH TO TACKLE CYBERCRIME

Inventions, discoveries, and new technologies widen scientific horizons but also bring new challenges for the legal world. Information Technology is brought by computers, computer networks, internet, and cyberspace. It also brought many new problems in jurisprudence. There was insufficiency of legislation while dealing with the information technology. Throughout the world the judiciary dealing with the new problem like cybercrime, adjudication and investigation of cybercrime, intellectual property Rights issues in cyber world etc. The United Nations Commission on Internet Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996.Model Law provides that all Nation should consider it, when they enact and revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper-based communication. Hence the most important enactment of the Bangladesh Information and Communication Technology Act, 2006 and Information and

Communication Technology (Amendment) Act, 2013 has been done (Sec. 4 of the information & communication Act, 2006). Cybercrime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation, and mischief, all of which are subject to penal laws of a country. The abuse of computers has also given birth to a gamut of new age crimes that are addressed by the special laws enacted to penalize these crimes. For example, in Bangladesh Tatha O Jogajog Projukty Ain 2006.

Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 defines certain offences which does not cover by the Penal Code. And so, it can be said that the Penal Code, 1860 is not effective enough in dealing with cybercrimes. The parliament of Bangladesh has enacted Information and Communication Technology Act, 2006 which defines certain activities as crime. The activities which made punishable under the Information and Technology Act of 2006 shall be the cybercrimes for the territory of Bangladesh. The activities are:

i. Mischief of computer and computer system
ii. Alteration of source code of commuter
iii. Hacking in computer system
iv. Publication of false, indecent, and defamatory statement or information in electronic form v.
v. Access in reserve system.
vi. False representation and concealment of information
vii. False electronic signature certificate.
viii. Transmission of secrecy
ix. Disclosing electronic signature for cheating.
x. Committing crime through computers.

**4.3 CYBER TRIBUNAL**

According to section 68 of the Information and Communication Technology Act, 2006 for the speedy and effective disposal of cases under this Act, Government shall establish one or more cyber tribunal. The tribunal shall try only the offences under this Act and the Government shall determine the local jurisdiction of the tribunal. In consultation with the Supreme Court, Government shall appoint on Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal. Cyber tribunal shall take a case for trial – a) Upon the report of a police officer not below the rank of sub-inspector or b) Upon a complaint made by a controller appointed under this Act or by any other person authorized by the controller

The trial procedure of cyber tribunal shall follow chapter 23 of Criminal Procedure Code, 1893 (Trial Procedure by the Court of Sessions) so far it is consistent. If the accused is absconded, tribunal can try the case in absentia. In this case tribunal has to circular an order in two Bangla newspapers to appear the accused on a specified date. Cyber tribunal shall apply the provisions of Criminal Procedure Code and it shall have the same power; a Sessions Court empowered to apply in its original jurisdiction. Public prosecutor shall conduct the case on behalf of the Government. Tribunal shall conclude

the trial within six months from the date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days.

## 4.4 CYBER APPELLATE TRIBUNAL

The Government shall establish one or more cyber appellate tribunal. The appellate tribunal shall be constituted by one chairman and two members appointed by the Government. To be appointed as a chairman of Cyber Appellate Tribunal, he must be either a former judge of the Supreme Court or existing judge of the Supreme Court or is eligible to be appointed as a judge of the Supreme Court. One of the two members of the tribunal shall be a retired District Judge or employed in the judicial service and the other member must be an experienced and skilled person in information and communication technology. They shall be appointed for 3-5 years. Cyber Appellate Tribunal shall have no original jurisdiction. It shall only hear and dispose of appeals from the order and judgment of the Cyber Tribunal and Sessions Court in appropriate cases. The decision of the appellate tribunal shall be final, and it shall have the power to alter, amend, and annul the order and judgment of the cyber tribunal. The appellate tribunal shall follow the appellate procedure of High Court Davison of the Supreme Court. Until cyber appellate tribunal is established, appeal may be heard by the High Court Division.

## 4.5 OVERALL OBSERVATION

It is undeniable that with the advance in the world, internet is becoming popular day by day and its use has rapidly expanded in Bangladesh. The growth of SNSs shows a significant change in the social behavior of Internet users because of some special features. It should not be disagreed that the several advantages of social networking through various ways as it develops social contract or relationship among the people (users), helps to enforce laws, such as law enforcement agencies may use SNSs to catch offender and to implement laws,[19] and spreads knowledge through sharing status. In many regards, Twitter has revolutionized modern communication, [20] as well as Facebook lies on the similar footing. Hundreds of thousands of their users are using these platforms every day to connect with others, to see others' views as well as to share their own views. Although there is important significance of SNSs in particular Facebook and Twitter as bearing a lot of benefits, the misuse of SNSs leading to cyber-crime including cyber defamation can also not be denied. Facebook and Twitter are playing role in committing as well as in preventing crimes. Hence, not only the use but also the users should be regulated in an acceptable manner. The importance of online social networks is not denied in any way. It is also not being said that the use of SNSs should be stopped or there should not be any right to express, but restriction on the use is being imposed through regulation. The basis is no one can exercise his or her right by



[19] Polices of one of the police station using Facebook officially as an informant sources of offences. Retrieved from https://www.Facebook.com/acpatroluttara.

[20] Kelley.(2013)

violating other rights, in other words, you have right to express anything but cannot harm others. How can the content of Facebook and Twitter in Bangladesh?

The court views on the defamatory statement or twibles statement made on online SNSs is positive in a sense as the trend is being changed through applying the laws on online environment.

Actually, judicial activism is very important to establish any cyber-crimes committed in cyber space. To some extent, Facebooking or twitting play a role as virus;[21] hence, legal instruments or directions can act as an antivirus to remove such virus acting in the form of cyber-crimes. Although there are national laws regulating cybercrimes including cyber defamation, the enactment of an international convention bears importance in order to harmonize such laws as it has become global issues on anonymous.

Apart from online anonymity i.e., the lack of need of identification complicating online defamation, extraterritoriality is another issue at global level. Alternatively, General Assembly of United Nation may introduce an international body by a resolution as it established the UNCITRAL in 1966 by a resolution 2205 (XXI).

Even if the output is a model law, it can also be fruitful as the UNCITRAL Model Laws on different subject matters are witnessing in the world. Moreover, now that no relevant international law exists and States have acted through enacting regulation but there is existence of various lacking, hence, the amendment of existing laws is needed. Lessig (2006) addressed four elements in order to control something, such as, laws, norms/policies, market, and architecture.[22] Before making any laws regulating cyber-crimes, these four things should be taken into consideration. Such amendment should contain satisfactory evidentiary standards, effective and strong enforcement mechanisms as law without enforcement is valueless. In order to do that, certain reforms of procedural laws especially of Bangladesh are needed. In Bangladesh, civil courts should be given a concurrent jurisdiction. As early stated, that there is very rear application of torts law in Bangladesh, and the tribunal established by virtue of section 68 of the ICTA 2006 only can impose imprison and fine as unlawful activities under present Act is treated as criminal offences, it should be given power to provide damages under the present laws. It is opined that civil remedy is better to get justice as the provision is balance of probability rather than criminal as it must be proved beyond reasonable doubt.



[21] in a seminar held in around 2006-2007 at a university situated in Bangladesh where Prof Dr. Mahtab Khanam, a well famous psychologist, was treating mobile phone as a virus due to misuse it very largely. In line with her thinking, I think Facebook is on same footing like mobile phone as technology/internet is cheapest and devices are easily portable

[22] Lessig, L. (2006). Code version 2.0. New York: Basic Books.

Chapter V

CONCLUSION AND RECOMMENDATION

## CONCLUSION AND RECOMMENDATION

Law is not only tool or forum to solve a problem. Apart from law, alternatively, distributed security approach to prevent cybercrimes including crimes in social networks can be adopted. Distributed security is a strategy to control cyber-crimes, and this new mode cannot rely on sanctions, but must instead turn the distributed nature of cybercrime on its head.[23] Distributed security approach can also be known as holistic approach.[24]Under this model, laws and law enforcement agencies are not sufficient to control any crime committed in cyber space. Hence, agencies, users, ISP and so on, have roles to play in controlling cybercrimes including cyber defamation. For example, ISP is considered as a door to access on the internet. They can set filters and help agencies to identify users who are misusing.

It is not said that the distributed security approach is only solution rather along with laws and policies, this new approach can also be adopted to control cyber-crimes.[25]Finally, legal framework of jurisdictions dealing with defamatory contents stands alone by themselves with similarities and differences between the two. Success of any law depends on how it is being implemented and how the people accepted it. If we all are ready to accept law, it will be successful. For effective and efficient implementation of legal regime, there must be a willingness to accept the spirit of the laws with its black letter.

## RECOMMENDATIONS



[23] Brenner, S. W. & Clarke+, L. L. (2005). Distributed Security: Preventing Cyber Crime. J. Marshall J. Computer & Info. L. 23. p.659.
[24] Asia Pacific Defense Forum. (2012). Cyber Evolution. USA. (37.1).
[25] Brenner & Clarke+.(2005).

**REFERENCE**


Asia Pacific Defense Forum. (2012).Cyber Evolution. USA. (37. 1).

Brenner, S. W. & Clarke+, L. L. (2005). Distributed Security: Preventing Cyber Crime. J. Marshall J. Computer & Info. L. 23. p.659.

Das, B. & Sahoo, J. S. (n.d.). Social Networking Sites-A Critical Analysis of Its Impact on Personal and Social Life. International Journal of Business and Social Science. (2.14). p. 222

Death Threat to PM on Facebook, Former BUET teacher gets 7yrs in jail.(2013, June 28). New Age (Online edn.)

European Network and Information Security Agency (ENISA). (2007, October). Securities Issues and Recommendations for Online Social Networks.

Fenn, L. M. (2006, November/December). Admissibility of Evidence: Information obtained from the internet. Tay& Partners.

Halsbury's Laws of England (4th ed.).

Islam, M. Z., & Jahan, A. (2015). RIGHT TO PRIVACY: IS IT A FUNDAMENTAL RIGHT IN BANGLADESH CONSTITUTION?. Journal of Asian and African Social Science and Humanities (ISSN 2413- 2748), 1(1), 1-7.

Islam, M. Z. (2013). Health as Human Rights under Malaysian National Legal Framework. IOSR Journal Of Humanities And Social Science (IOSR-JHSS) Vol.12(5), 51-57

Kwasniewski, B. W. (2011, March 30). Social Media: An Emerging Issues in the Workplace. Charity Law Bulletin. 246

Kelley, B. J. (2013). Tortious Tweets: A Practical Guide to Applying Traditional Defamation Law to Twibet Claims. Louisiana Law Review. 73. p.559.

Kumar, R. (2009, November 6). Cyber Defamation- Position in India.

Lessig, L. (2006). Code version 2.0. New York: Basic Books

Munir, A. B. & Yasin, H. M. (2010). Information and Communication Technology Law: State, Internet and Information; Legal and Regulatory Challenges. Selangor: Sweet & Maxwell Asia.

MIRGEN, P. (n.d.). Defamation in Cyber Space", Curentul Juridic. p.97

Nicolos, E. (2010). A Practical framework for preventing mistrial by twitter. Cardozo Arts & Entertainment. 28. p.385

Rahman, M. S. (2013). Cyber Crime, Cyber Security and Bangladesh

Stephenson, P. (2007). Cyberlaw in Hong Kong(2 nd edn.). Hong Kong: LexisNexis.

Townsend, A. M., Aalberts, R. J. & Gibson, S. A. (2000). Libel and Slander on the Internet. Communication of the ACM. (43.6). p.15.

Vamialis, A. (2013). Defamation: Confronting Anonymity. International Journal of Law & Information Technology. (21.1). p.31.