

## **Offensive Statements on Social Networking Platforms with the special reference to Cyber Defamation: A Comparative Analysis between Malaysia and Bangladesh**

**Shahin Alam\*,<sup>1</sup> Md. Zahidul Islam<sup>2</sup>**

<sup>1</sup>*Postgraduate Student, Ahmad Ibrahim Kulliyah (Faculty) of Laws (AIKOL), International Islamic University Malaysia (IIUM).*

<sup>2</sup>*PhD Researcher, Ahmad Ibrahim Kulliyah (Faculty) of Laws(AIKOL), International Islamic University Malaysia (IIUM).*

---

### **ABSTRACT**

---

#### **Keywords:**

*Social Networking;  
Cyber Defamation;  
Bangladesh and  
Malaysia.*

Crimes committed due to misuse of social networking sites are becoming a serious matter in Malaysia, Bangladesh as well as whole over the world. As a comparative 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 as well as Malaysia, 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 Malaysia as well as Bangladesh through Facebook & Twitter.

---

**Publisher All rights reserved.**

---

## INTRODUCTION

There is a growing popularity of Social Networking Sites (SNSs) among the Internet users. At present, 1.5 billion people across the world have their profiles in social networking sites.<sup>i</sup> Recently, both Malaysia and Bangladesh have seen a phenomenal increase in the use of SNSs such as personal blogs, Facebook and Twitter. Facebook has about 1.11 billion monthly active users worldwide,<sup>ii</sup> and estimated 500 million people are using Twitter.<sup>iii</sup> There are about 13.3 million Facebook users in Malaysia which representing almost 46 percent of its total population, and this puts Malaysia on the 8th spot in Asia and 21st place in the world.<sup>iv</sup> Statistics show almost 2 million people use Twitter in Malaysia.<sup>v</sup> In compare with, approximately 3.4 million Bangladeshi use Facebook which is about one-fourth of Malaysian Facebook users,<sup>vi</sup> and no authentic source of statistics regarding Tweeter users in Bangladesh is found, but it cannot be said that Twitter is not gaining popularity in this territory. It is believed that the number of users of both SNSs in both jurisdictions as well as whole over the world is being increased. The popularity of Social Networking Sites particularly Facebook and Twitter is undeniable as the number of their users is growing day by day as they offer their members the ability to connect instantly and communicate with other members. However, various types of cyber crimes are being committed by using Facebook or Twitter. This paper examines how referred SNSs are being misused by their users through making offensive statements.

## CONCEPTUAL DEFINITIONS

### **Social Networking**

Online Social Networks or Social Networking Sites (hereinafter called SNSs) are one of the most remarkable technology phenomena of the 21st century.<sup>vii</sup> It can be broadly defined as “social media or social network is an online social structure made up of individuals or organizations, which permits easy online interaction by users”.<sup>viii</sup> It enables people to socially interact with one another online. Facebook, Twitter, LinkedIn, and MySpace are more popular social networking websites in the world, and among them Facebook and Twitter are considered as the top SNSs. From the number of users, it can be realized that the most popular SNSs is

Facebook which was launched in February 2004, operated and privately owned by Facebook, Inc.<sup>ix</sup> Facebook provides online social networking service, and it allows its users to create personal profiles, and the users can connect instantly with one another, to upload or download and share links. Twitter is also another very popular online SNSs or online application which was launched in 2006.<sup>x</sup> Twitter is commonly described as a 'social networking and micro-blogging tool', which allows members (also called tweeters) to send and read 140 characters text messages, regarding latest stories, ideas, opinion, and news, known as 'tweets'.<sup>xi</sup> The term twibelis used to describe libelous statements posted on Twitter.<sup>xii</sup>

### **Cyber Crimes**

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.<sup>xiii</sup> 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.

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 anti-social 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.

### **Offensive statements**

Offensive statement means any statement can lead to an offence. It includes defamation, hate speech, statement making against the State or authority or any religion or belief. Generally, a statement is considered as defamatory if it "tends so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."<sup>xiv</sup> A defamatory statement is also defined as "a statement which attempts to lower a person in the estimation of right-thinking members of society generally or to cause him to be shunned or

avoided or to expose him to hatred, contempt or ridicule, or to convey an imputation on him disparaging or injurious to him in his office, profession, calling, trade or business”.<sup>xv</sup>Defamation can take in the form of libel (printed defamation) or slander (spoken defamation).<sup>xvi</sup>A defamatory statement may be in the form of words, pictures, visual images, gestures or any other method which signify a meaning.<sup>xvii</sup>

Cyber Defamation occurs when defamation is committed with the help of computers or the Internet, for instance, someone publishes any defamatory matters about someone on any online platform.<sup>xviii</sup> In other words, “any act, deed, word, gesture in cyberspace designed to harm a person’s reputation on the internet amounts to defamation”.<sup>xix</sup>With the advance of social network system, cyber defamation is now easier than making a defamatory statement in real world. The reason is SNSs like Twitter and Facebook permit to publish or post a statement instantly that can reach thousands of people. Online defamation is treated the same way as more traditional forms irrespective of posting in blog, or updating status in Facebook or Twitter, that is to say, action can be taken against makers of such a post or update for any defamatory statements posted or updated online.

## LEGAL FRAMEWORKS

### **Legal Regime in Malaysia**

The Computer Crimes Act 1997 (CCA) actually modeled from the UK’s Computer Misuse Act 1990 is the prime legislation which was enacted to control cyber crimes in Malaysia, for example, unauthorized access or unauthorized modification are considered as cyber crimes in law.<sup>xx</sup>For the purpose of ensuring the protection against the misuses of computers and computer criminal activities the present Act was made, but it is silent on making offensive statement on online platforms including cyber defamation committed by using computer. In order to regulate defamation committed in cyber space more specifically in Facebook and Twitter platforms, the Malaysian Communication and Multimedia Act 1998(herein after called CMA) is relevant. The objectives of the CMA is to regulate the converging communications and multimedia industries, and for incidental matters.<sup>xxi</sup>

Section 211 of the CMA 1998 prohibits offensive content in online environment. According to the present section, if the content applications service provider, or other person using a content applications service shall not provide content which is indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person, shall be treated as an offence, and shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding RM 50,000 or to both. It further states that if such convicted person continues in committing same offence, he shall be liable to a further fine of RM 1000 for every day during which the offence is continued after conviction.

Additionally, section 233 of the CMA 1998 imposes prohibition on improper use of network facilities or network service. The use of network facilities or network services in an inappropriate manners stated in the present section is an offence under section 233 and will be punished with same punishment as mentioned for offence under section 211.<sup>xxii</sup> In order to constitute an offence under section 233, by means of any network facilities or network service or applications service knowingly

- a. making or soliciting, and initiating the transmission of any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person; or
- b. Initiating a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address; or
- c. Providing any obscene communication for commercial purposes to any person; or permitting a network service or applications service under the person's control to be used for an activity described in section.

Moreover, the Penal Code, as a general substantive criminal law in Malaysia, treats defamation as an offence in chapter XXI (sections 499-502). Defamation prescribed in section 499 of Penal Code is punishable with imprisonment for a term which may extend to two years or with fine or with both.<sup>xxiii</sup> Malaysian Penal Code was borrowed from Indian Penal Code which was drafted in the line of principles laid down in English criminal laws. Section 40 states that any offences inserted in any other laws are also subject to chapter 'IV of PC',<sup>xxiv</sup> unless otherwise directs expressly. In addition, action can also be taken for any defamatory matters under 'tort'<sup>xxv</sup> law in Malaysia.

In order to establish successfully a prima facie case of defamation in court of law, the following four elements are generally required:<sup>xxvi</sup>

- a. that the statement was made by the defendant;
- b. that statement was published to one other than the person defamed;
- c. that the statement was false referring to, and tending to harm the reputation of the plaintiff; and
- d. that the statement was unprivileged.

### **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 in 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.<sup>xxvii</sup>

Moreover, the Penal Code 1860, a general criminal law, also 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 an punishable offence. Additionally, in the legal system of Bangladesh it is also open for the defamed person to take action under tort law, and claim damages for making and publishing any defamatory statement.

#### BRIEF CASES ANALYSIS

##### **Malaysian Scenario**

*Dato' Mohamad Salim Fateh bin Fateh Din v Nadeswaran a/l Rajah (No 1)*<sup>xxviii</sup>The plaintiff, a prominent businessman, sued the defendant, a well-known columnist, for publishing two defamatory statements made about him on Twitter. One of them was “The land thief is trying intimidation! I love a good battle! War is now declared. I’ll take him on”. The plaintiff argued the postings made by the defendant could be read by anyone who accessed his website, and he had thousands of followers of his Tweets, among them prominent corporate figures, politicians and media personalities. The plaintiff said the defamatory statements damaged his reputation and caused him extreme embarrassment and distress. As a result, the plaintiff claimed damages including aggravated damages and an injunction to restrain defendant from further publishing or causing to be published any similar words defamatory. No defense was filed by the defendant; hence, the case was decided ex parte.

The defendant was ordered to pay total RM 500,000 (£101,000) damages by the High court in Kuala Lumpur, and an injunction against the defendant was granted to refrain from further publishing the defamatory statements or any similar defamatory statements. As the defendant has served no defense, he was deemed to have admitted all averment as contained in the plaintiff’s statement of claim. In considering the amount of damages to be awarded in light of the defendant’s conduct in failing to apologize and to withdraw the offending statements from his website which remained there right up to the date of the hearing,<sup>xxix</sup> the Judge stated that the defendant had more than 4,000 followers and any number of casual drop ins would naturally see heavy traffic and “the court is thus of

the view that the defendant should exercise a greater degree of care over his tweets knowing full well that it could and would be seen by many”.<sup>xxx</sup> In Malaysia, this is the first Twitter defamation claim and a landmark case where online defamation was justified by the court of law. This case was covered in various news reports in Malaysia, in particular, in the ‘Sun Daily’ and the ‘Star’ in the form of a comment ‘Think before you Tweet’.<sup>xxxii</sup> The attitude of Malaysian court is very positive in respect of the defamation on online platforms. It might be argued that by this decision the right to freedom of speech is being restricted, but it must be borne in mind that the freedom of speech on online must not unreasonably and adversely affect another person’s well-being and interests, like to the physical world.<sup>xxxiii</sup> If the appeal was preferred, judgment debtor might argue on the ground of essential requirements to establish a defamatory claim. As it was made by higher judiciary, it is still a binding decision as no appeal was preferred.

*National Union of Bank Employees v NoorzeelabintiLamin and Anor*<sup>xxxiii</sup> In this case some defamatory comments were published to all the defendant's friends on Facebook and also to all others who could have access to view the defendant's Facebook page. The plaintiff case was that by reading comments made by the defendants, anyone would think that the plaintiff is a dishonest union who cheats its members; that the plaintiffs are all dishonest and have their own agenda; that the plaintiff does not pay its members from the Benevolent Fund; that the plaintiff's misappropriates the monies; and that the plaintiffs are corrupt; that the plaintiff is incompetent in serving its members. Therefore, the plaintiff argued that their reputation was damaged due to making these comments, and claimed damages.

The court ordered to pay damages as well as granted an order restraining the defendants from publishing and/or causing to issue similar libels in future. On defamatory statements on Facebook webpage, the Court opined that “...this is equally serious. In this day of social media networking, a comment posted on one's Facebook page has the ability to reach a large number of persons in a short space of time. The comments of the defendant which are read by her Facebook friends can in turn be read by their friends, depending on the privacy settings”.<sup>xxxiv</sup> After due consideration of the evidence adduced by both parties, the Court found that the plaintiff has succeeded in making out its case against the defendants on a balance of probabilities.

### **Bangladesh scenario**

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 *ex parte* as he didn't 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.<sup>xxxv</sup> 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 27<sup>th</sup> 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.<sup>xxxvi</sup> 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.<sup>xxxvii</sup> In all of the stated cases brought before the 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 write-ups and hurting religious sentiments in online platforms (for hurting religious sentiments).<sup>xxxviii</sup> 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.<sup>xxxix</sup> 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.

### COMPARATIVE ANALYSIS

European Council's Convention on Cyber Crime 2001 is the first international treaty on crimes committed via the Internet. It is not a global convention, but considered as a regional treaty although some Non-European countries are parties to it. It is only one convention bearing international characters on cybercrimes. Although the convention provides a legal framework for the protection of society against cyber crime, it is silent on making offensive statement particularly cyber defamation as they are more concerned on cyber crimes in serious nature. Hence, it may be



difficult to analyze and evaluate the issues relating to defamation in cyber space in the light of international legal provisions. The national constitutions of both jurisdictions guarantee freedom of speech and expression as a conditional human right.<sup>xi</sup> It is also recognized no one can violate the rights of others in the exercise of his or her rights.<sup>xii</sup> It is undeniable that defamation is being committed in online social networking websites particularly in Facebook and Twitter through making or posting statements defaming others or hurting religious sentiment of others, therefore, Malaysian CMA 1998 and ICTA 2006 of Bangladesh are relevant to analyze and examine for this paper. Moreover, the Penal Code and Tort law of both jurisdictions are also come within the purview of present evaluation.

### Legislative Stance

Both of the territories have enacted regulations to control cyber crimes including defamation in cyber space. In Bangladesh, among others, the defaming information in electronic form is considered serious offences as per the amendments made in 2013 as punishment for defamatory statement has been increased showing its seriousness.<sup>xiii</sup> The present cyber law of Bangladesh also authorizes law enforcement agencies to arrest the alleged offender without warrant. However, Malaysian stance is better comparatively as they are trying to remove legal obstacles on the relevant issues through making amendment in relevant substantive as well as procedural legal frameworks.

In Bangladesh, the provision of section 57 of ICTA covers online defamation including defamation in Facebook and Twitter as the terms "...in the websites or in the electronic form...." have been used in present provisions. Similarly, defamatory statements used in any SNSs will be treated as an offence under section 211 or/and 233 of CMA in Malaysia. 'Sedition'<sup>xliii</sup> in the terms of 'prejudice the image of the State', and hate law or law protecting religious sentiment in the terms of 'causes to hurt or may hurt religious belief' are covered under the same provisions of the ICTA of Bangladesh, unlike Malaysia as they have separate regulations dealing with these, that is, the Sedition Act 1948. A person found guilty of sedition under this Act may be imprisoned to three years in jail, or to fine RM 5,000, or both.<sup>xliv</sup> It criminalizes speech with seditious tendency,<sup>xlv</sup> and it is immaterial to constitute an offence whether seditious statement is true or false.<sup>xlvi</sup> The most recent charge framed under this Act is the case of the five speakers in a particular forum and a woman who allegedly spoke against the Yang Di-Pertuan Agong on Facebook.<sup>xlvii</sup>

Both Bangladesh and Malaysia adopted Indian Penal Code set out same provisions regarding criminal defamation still bearing the same punishment. To control the said issues, both jurisdictions made special laws which prevail on general law. If defamation is committed in any online platform and if it is not possible to take action due to certain deficiencies in special one, criminal action can be taken against the offender under the Penal Code as it does not mention any platforms to

constitute defamation. There is no specific ‘blasphemy law’<sup>xlviii</sup> in both territories, but they curbs blasphemy and any insult to any religion by the provisions of the Penal Code as it provides penalties for offenses against religion.<sup>xlix</sup> Additionally, Malaysia punishes such transgression with *Shariah* when applicable. Hence, any statement in online platform including Facebook and Twitter made against Islam as well as any religion is punishable under several laws of Malaysia and Bangladesh.

Legislative position of both jurisdictions is positive; undoubtedly these are good trend to control crimes in cyber space. However, these are not loopholes free. Although the purpose of the CMA is hard i.e. to prevent this type of serious crime the CMA was made, by using the terms ‘with intent to annoy.....’ in relevant provisions of the CMA, it became soft in nature. Due to use these terms, defamatory statements’ makers or publishers will try to take chance of doubt from those, on the other hand, the relevant provision of the ICTA does not incorporate these types of terms in respect of the defamatory issues.<sup>1</sup>

Another issue is that both the CMA and the ICTA incorporate the provisions of extraterritorial jurisdiction as these are supposed to be applied to crimes committed all over the world,<sup>li</sup> but it is unknown how this can be achieved in practice.

Moreover, ISP stands for Internet Service Provider facilitates internet services. Without their facilitation, no commission of crime is possible as they have control on internet content. Although, section 233 does not mention ISP’s name, it implies ISP’s liability as it has used the term ‘...who permitting a network service.....’.<sup>lii</sup> Similarly, in section 114A of Evidence Act 1950 Malaysia the words ‘who in any manner facilitates to...’ are used which indicates ISP’s liability, whereas, Bangladeshi law is silent on this issue. It is not ambiguity free as there is no express and direct provision as to ISP liability. ISP should also carefully consider potential exposure to defamation actions when they offer any kind of content service. Such services attract customers, but may also expose the otherwise exempt ISP operator to defamation lawsuits if not carefully monitored.<sup>liii</sup>

### **Enforcement Mechanisms**

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.

Section 114A of Malaysian Evidence Act 1950 deals with burden of proof of online publications. Unlike the principle of presumption of innocence, it lays down that the accused will be presumed guilty until otherwise proved, hence, burden of proof lies on accused. In order to encourage easier and speedy enforcement of laws, section 114A was inserted in the evidence law. Issue is whether information from internet is document or not? Sections 90A, 90B and 90C of Evidence Act of Malaysia deals with admissibility of information obtained from the internet. Section 90A & explanation 3 of section 62 says that a document produced by a computer or statement contained in such documents, during ordinary course of its use, is a primary evidence. The present provision does not say about computer printout (printout information from internet). However, the 'internet' will come under definition of 'computer' given in law as it being a device for storing information as the terms "...that whatever name or description such device is called" have been used in definition of computer.<sup>liv</sup>

The ICTA made electronic data produced by computer, for example, e-mails as admissible evidence,<sup>lv</sup> 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".<sup>lvi</sup> Whether online platform is a substance or not is an unsettled issue. Moreover, it is difficult to state from various explanations and illustrations of Evidence Act as well as from legislative background that legislature intended to consider e-information as evidence, that's why Malaysia inserted the specified sections. Due to facing similar problems, India also inserted section 65B in its evidence law which recognizes electronic records as admissible evidence.

### **Judicial Views**

In 2006, an English court in *Keith-Smith v Williams* confirmed that the existing libel law applies on net.<sup>lvii</sup> Similarly, the attitudes of judiciaries of Malaysia and Bangladesh are 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 Malaysian 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 the judiciary of Bangladesh. Malaysia and Bangladesh are both common law countries and adopted tort law from English laws. By virtue of sections 3 & 5 of Civil Law Act 1956, English law is applicable in Malaysia subject to certain provisions.

Though there is no binding authority, the courts of Bangladesh also follow English rule as persuasive authority. From the judicial cases, it could be realized that the cases come before the Malaysian courts due to misuse of social networks mostly under tort law, but 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 Malaysia by judicial precedents, that is to say, some cases have already been decided by the High Courts. The cases brought before higher judiciary in Malaysia who makes binding precedent, unlike Bangladesh scenario. In Bangladesh, the trend to come before the court on said issues are started recently and almost 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 Malaysian 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.<sup>lviii</sup> In the case of *Ayob bin Samad v TS Sambanthamurthi*, Mohamed Dzaidin 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.<sup>lix</sup> If the statement is true, the person against whom statement was published doesn't 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.

## FINAL OBSERVATIONS

It is undeniable that with the advance in the world, internet is becoming popular day by day and its use has rapidly expanded in Malaysia as well as Bangladesh. The growth of SNSs shows a significant change in the social behavior of Internet users because of their 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,<sup>lx</sup> and spreads knowledge through sharing status. In many regards, Twitter has revolutionized modern communication,<sup>lxi</sup> 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 violating others rights, in other words, you have right to express anything but cannot harm others. How can the content of Facebook and Twitter in Bangladesh and Malaysia be regulated? How can we control offensive statement including cyber defamation committed due to misuse of SNSs?

The court views on the defamatory statement or twibelous 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;<sup>lxii</sup> hence, legal instruments or directions can act as an anti-virus to remove such virus acting in the form of cyber crimes. Although there are national laws regulating cyber crimes including cyber defamation, the enactment of a 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 taken action 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.<sup>lxiii</sup> 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 Malaysia, 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.

Digital natives are not aware about the effect of misuse, even they don't want to approve their work as a crime, and they want free use of internet without regulation. To increase awareness among the users and others that any forms of cyber crimes including making offensive statement on online is a crime as it is anti-social, it is harming others, and you might also be affected by others. Without creation of awareness among the users about cyber crime, control is tough as the technology is being developed everyday rapidly.

It is also necessary in both jurisdictions to make clear by establishing legal provisions to regulate who exactly will be held responsible for defamatory statement. It is thought that the liability of ISPs should be enhanced. They should be regulated and monitored properly as they have editorial control over the publication of defamatory statement. They can be watched by an authority which might be established to act as watchdog. The Bangladesh Telecommunication Regulatory Commission (BTRC) already has set up a cybercrime watchdog unit to monitor harmful content or activities on the Internet including SNSs and mobile platform.<sup>lxiv</sup> Furthermore, it is mentioned in the policy of SNSs including Facebook policy and Terms of Service of Twitter,<sup>lxv</sup> that “users will not post content or take any action that infringes or violates someone else's rights or otherwise violates the law....., and that responsibility lies on one who originated such offensive content.....”<sup>lxvi</sup> Unsettled question is by inserting these provisions whether they can be exempted from their liability of monitoring and removing illegal contents. Apart from those, as mentioned earlier that one of the universal problems as to cyber crimes also relevant to crimes due to misuse of social network is anonymity.<sup>lxvii</sup> Although there is an IP address to identify user and place of use, the use of internet in cyber café is still an issue. Bangladesh has initiated a measure by issuing an announcement to cyber café service provider to collect name and address of users. Law enforcement agencies of Bangladesh having no proper knowledge on enforcement of cyber crimes law, therefore, the government is planning to provide proper training to them. It is also suggested that the judiciary must be trained to evaluate possible harmful effects of social media.<sup>lxviii</sup>

Law is not only tool or forum to solve a problem. Apart from law, alternatively, distributed security approach to prevent cyber crimes 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 cyber crime on its head.<sup>lxix</sup> Distributed security approach can also be known as holistic approach.<sup>lxx</sup> 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 cyber crimes including cyber defamation. For example, ISP is considered as a door to access in 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.<sup>lxxi</sup>

Finally, legal framework of both 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.

<sup>i</sup> 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). 222. Retrieved from www.ijbssnet.com

<sup>ii</sup> Retrieved from <http://www.quintly.com/blog/2013/05/Facebook-country-statistics-may-2013/> (2013, November 15)

<sup>iii</sup> Retrieved from <http://www.telegraph.co.uk/technology/Twitter/9945505/Twitter-in-numbers.html> (2013, November 12); Retrieved from <http://www.mediabistro.com/allTwitter/tag/total-Twitter-users>(2013, November 12)

<sup>iv</sup> Retrieved from <http://www.theborneopost.com/2013/06/16/13-3-million-msians-are-Facebook-users/>(2013, December 31)

<sup>v</sup> Retrieved from <http://www.forest-interactive.com/Twitter-users-2013/>(2013, November 12)

<sup>vi</sup> Retrieved from <http://wearesocial.net/tag/statistics/>(2013 November 12)

<sup>vii</sup> European Network and Information Security Agency (ENISA).(2007, October). Securities Issues and Recommendations for Online Social Networks. p.3. in Munir, A. B. & Yasin, S. H. (2010). *Information and Communication Technology Law: State, Internet and Information; Legal and Regulatory Challenges*. Selangor: Sweet & Maxwell Asia. p.83.

<sup>viii</sup> Kwasniewski, B. W. (2011, March 30). Social Media: An Emerging Issues in the Workplace. *Charity Law Bulletin*, 246.

<sup>ix</sup> Retrieved from www.wikipedia.com

<sup>x</sup> Kwasniewski. (2011).

<sup>xi</sup> Nicolos, E.(2010). A Practical framework for preventing mistrial by Twitter. *Cardozo Arts & Entertainment*. 28. p. 385.

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

<sup>xiii</sup> Retrieved from <http://www.mondaq.com/india/x/28603/technology/Cyber+Crimes+an+unlawful+act+where+in+the+computer+is+either+a+tool+or+a+target+or+both>> (2014, January 1)

<sup>xiv</sup> Kelley. (2013).

<sup>xv</sup> *Halsbury's Laws of England*. (para. 10, p. 7.). (4<sup>th</sup> ed.).

<sup>xvi</sup> Kelley (2013) quoted it by referring other sources.

<sup>xvii</sup> Stephenson, P. (2007). *Cyberlaw in Hong Kong*. Hong Kong: LexisNexis. p.51.

<sup>xviii</sup> Rahman, M. S. (2013). Cyber Crime, Cyber Security and Bangladesh. Retrieved from <http://teletechblog.blogspot.com/2013/05/cyber-crime-cyber-security-and.html>

<sup>xix</sup> Kumar, R. (2009, November 6). Cyber Defamation-Position in India. Retrieved from <http://jurisonline.in/2009/11/cyber-defamation-%E2%80%93-position-in-india/>

<sup>xx</sup> The Computer Crimes Act 1997. ss.3 & 5.

<sup>xxi</sup> The Communication and Multimedia Act 1998. Long title.

<sup>xxii</sup> *Ibid.* s. 233(3).

<sup>xxiii</sup> The Penal Code. s. 500.

<sup>xxiv</sup> Chapter IV of Penal Code lays down about general defenses or general exceptions of offences prescribed in the Code.

<sup>xxv</sup> Tort is a civil wrong where remedy is only damages (monetary compensation). It must not be confused that in Malaysia, basically the principles of tort are taken from English law, but not from French tort law.

<sup>xxvi</sup> Retrieved from <http://injury.findlaw.com/torts-and-personal-injuries/elements-of-libel-and-slander.html#sthash.fTWUgMF0.dpuf> (2013, December 19).

<sup>xxvii</sup> 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 cyber crimes was increased by setting a minimum of seven years imprisonment and a maximum of 14 years or a fine of Tk 1 crore or both.

<sup>xxviii</sup> [2012] 10 MLJ 203; [2012] MLJU 391.

<sup>xxix</sup> *Dato' Mohamad Salim Fateh bin Fateh Din v Nadeswaran a/l Rajah* (No 1) [2012] 10 MLJ 203; [2012] MLJU 391, at para 63.

<sup>xxx</sup> *Ibid.* para 64.

<sup>xxxi</sup> Retrieved from <http://inform.wordpress.com/2012/04/29/malaysia-journalist-ordered-to-pay-100000-damages-in-Twitter-libel-case/> (2013, December 21)

<sup>xxxii</sup> Retrieved from <http://www.greyreview.com/2012/04/27/first-malaysian-ordered-by-court-to-pay-rm500000-libel-damages/> (2014, January 1).

<sup>xxxiii</sup> [2013] MLJU 531.

<sup>xxxiv</sup> *Ibid.* para. 149.

<sup>xxxv</sup> 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).

<sup>xxxvi</sup> *Ibid.*

<sup>xxxvii</sup> The report was published on 10<sup>th</sup> February 2014 in bangle in <http://tazakhobor.com>

<sup>xxxviii</sup> Retrieved from <http://www.globaltimes.cn/content/809498.shtml#Ur1i4VGczIU> (2013, November 20)

<sup>xxxix</sup> The news of this stay proceedings was published on 16<sup>th</sup> February 2014 in bangle in <http://www.banglanews24.com>

<sup>xl</sup> The Constitution of the People's Republic of Bangladesh 1972, art. 39; The Federal Constitution of Malaysia 1957, art. 10.

<sup>xli</sup> The Universal Declaration of Human Rights, art. 29(2).

<sup>xlii</sup> ICT (Amendment) Act 2013, s. 57.

<sup>xliii</sup> [Informally, it may be known as defamation](#) against government or State. A definition of sedition found as the conduct or language inciting rebellion against the authority of a state. It is considered a subversive act, and the [overt acts](#) that may be prosecutable under sedition laws vary from one legal jurisdiction to another. Retrieved from <http://www.freemalaysiatoday.com/category/opinion/2013/07/21/how-to-avoid-being-seditious/>

<sup>xliv</sup> The Sedition Act 1948, s. 4(1).

<sup>xlv</sup> Retrieved from <http://www.freemalaysiatoday.com/category/opinion/2013/07/21/how-to-avoid-being-seditious/> (2014, December 1).

<sup>xlvi</sup> *PP v Oh Keng Seng* [1978].

<sup>xlvii</sup> Retrieved from <http://www.freemalaysiatoday.com/category/opinion/2013/07/21/how-to-avoid-being-seditious/>

<sup>xlviii</sup> Wikipedia defines it as a [law](#) limiting the freedom of speech and expression relating to [blasphemy](#), or irreverence toward holy personages, religious artifacts, customs, or beliefs. This law forbids [hatespeech](#) or religious insult.

<sup>xlix</sup> The Malaysian Penal Code, ss. 295-298A; The Bangladesh Penal Code, ss. 295-298, both deal with offences against religion.

<sup>i</sup> The CMA, ss. 211 & 233; The ICTA, s. 57.

<sup>ii</sup> The CMA, s. 4(1); The ICTA, s. 4(1).

<sup>iii</sup> The CMA, s. 233(2).

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



- <sup>liv</sup> Fenn, L. M. (2006, November/December). Admissibility of Evidence: Information obtained from the internet. *Tay& Partners*. Retrieved from [www.taypartners.com.my](http://www.taypartners.com.my)
- <sup>lv</sup> The ICTA. s. 13.
- <sup>lvi</sup> The Evidence Act 1872. s. 3.
- <sup>lvii</sup> Retrieved from <http://www.theguardian.com/media/2006/mar/23/digitalmedia.law> (2014, January 2)
- <sup>lviii</sup> Retrieved from <http://injury.findlaw.com/torts-and-personal-injuries/elements-of-libel-and-slander.html#sthash.fTWUgMF0.dpuf> (2013, November 11)
- <sup>lix</sup> [1989] 1 MLJ 315; [1989] 1 CLJ 152; [1989] 1 CLJ (Rep) 321; See also *Dato' Seri Mohammad Nizar Bin Jamaluddin v Sistem Televisyen Malaysia Berhad & Anor* [2013] MLJU 272.
- <sup>lx</sup> Polices of one of the police station using Facebook officially as an informant sources of offences. Retrieved from <https://www.Facebook.com/acpatroluttara>.
- <sup>lxi</sup> Kelley.(2013).
- <sup>lxii</sup> 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.
- <sup>lxiii</sup> Lessig, L. (2006). *Code version 2.0*. New York: Basic Books.
- <sup>lxiv</sup> Retrieved from <http://www.zdnet.com/bangladesh-sets-up-cybercrime-watchdog-2062303622/> (2014, January 1).
- <sup>lxv</sup> Facebook website. Policy 5; Twitter website. Terms of Service.
- <sup>lxvi</sup> Facebook website. Policy 5.
- <sup>lxvii</sup> Vamialis, A. (2013). Defamation: Confronting Anonymity. *International Journal of Law & Information Technology*. (21.1). p.31.
- <sup>lxviii</sup> Nicolos. (2010).
- <sup>lxix</sup> Brenner, S. W. & Clarke+, L. L. (2005). Distributed Security: Preventing Cyber Crime. *J. Marshall J. Computer & Info. L.* 23. p.659.
- <sup>lxx</sup> Asia Pacific Defense Forum. (2012). Cyber Evolution. USA. (37.1).
- <sup>lxxi</sup> Brenner & Clarke+. (2005).

## REFERENCES

- 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* (4<sup>th</sup> 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<sup>nd</sup> 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.