Cybercrime in the social media of Bangladesh: an analysis of existing legal frameworks

Article *in* International Journal of Electronic Security and Digital Forensics · January 2022

DOI: 10.1504/IJESDF.2022.119998

2 authors, including:

Kudrat-E- Khuda Babu
Daffodil International University
23 PUBLICATIONS **68** CITATIONS

SEE PROFILE

Cybercrime in the social media of Bangladesh: an analysis of existing legal frameworks

Kudrat-E-Khuda Babu*

Department of Law,
Daffodil International University,
Dhanmondi, Dhaka-1207, Bangladesh
Email: kekbabu.law@diu.edu.bd
Email: kekbabu@gmail.com
*Corresponding author

Md. Abu Bakar Siddik

Department of Law,
Comilla University,
Comilla, Bangladesh
Email: absmasum.cu09@gmail.com

Abstract: Unprecedented and rapid expansion of ICT has meant it has become a common platform for prospective criminals intending to commit crimes in a non-traditional manner. These new-age crimes are popularly known as cybercrimes in the form of stalking, hacking, cyber obscenity, cyber theft, breach of confidentiality, etc. The rampant growth of IT has pushed the legislators of developing countries like Bangladesh into various challenges and difficulties in moulding new legal regimes to govern the virtual world from multiple types of cyber problems. Now cybercrime in social media is in a state of flux, which not only demands adequate tools to combat this but also requires terminological clarification of particular conduct as cybercrime or not. The paper attempts to depict several sorts of cybercrime in cyberspace, particularly in social media. It also examines existing regulations in light of current issues using data analysis of acquired samples from specific locations to anticipate clever minds of possible cybercriminals.

Keywords: Bangladesh; cybercrime; information technology; legal framework; online; social media.

Reference to this paper should be made as follows: Babu, K-E-K and Siddik, M.A.B. (2022) 'Cybercrime in the social media of Bangladesh: an analysis of existing legal frameworks', *Int. J. Electronic Security and Digital Forensics*, Vol. 14, No. 1, pp.1–18.

Biographical notes: Kudrat-E-Khuda Babu is the Head of the Law Department at Daffodil International University, Bangladesh; an international member at Amnesty International; Climate Activist at Greenpeace International and a columnist. Besides, he is an associate member at the Centre for the Study of Global Human Movement, University of Cambridge. Moreover, he is a Visiting Professor at the Lyceum of Philippines University-Laguna. He has published articles and book reviews in different journals including the journals of Oxford University and Cambridge University. He is in the editorial board of nine peer-reviewed and Scopus indexed journals from the UK, Canada, India, Turkey, Saudi Arabia, and the USA.

Md. Abu Bakar Siddik is an Assistant Professor and the Chairman of the Law Department at Comilla University, Comilla, Bangladesh. He served as a House Tutor at Bangabandhu Hall (students' dormitory) and is a member of the academic council at the same university. He also served as a Student Adviser under the Law Department of his working university. He completed his graduation and post-graduation from the Law Department of Chittagong University, Bangladesh. His research areas focus on cyber law, family law, and environmental law.

1 Introduction

Every single person using internet nowadays uses social networking sites (SNSs). Social media has become a platform for every kind of communication. Every single person using internet nowadays uses SNSs. Social media has become a platform for every kind of communication

Nowadays often every internet user operates SNSs as their tools of communication and social media has become a common platform for often every type of internet communications (Nahar and Minar, 2018). It has made our society more compact and our relations to each other more condensed (Ullah, 2019). With the advent of information technology (IT), our life has become easier and also made crime easier too. IT obliterates the need for actual physical contact to commit the crime and this paves the way of maintaining anonymity by cybercriminals. The intrusion and proliferation of computer-based programs into often every sphere of our life have widened the opportunity for perpetrators so many forms of committing crimes that had never been possible previously.

This created some latest and highly modernised facilities and options for sinister to break the law which are technically known as cybercrime. Such crime has assumed a very wide implication where everything in our life from the microwave oven to the nuclear power plant is being run on computers (Karzon, 2008). This term being a multidimensional concept creates a myriad of iceberg situations as there is no coherent, consistent and concurrently formulated connotation. Bangladesh responded to cyber problems in early 2006 by putting in place the Information and Communication Technology (ICT) Act, 2006 which by the phase of time also, become inadequate. Very recently to accelerate justice for cybercrime victims and to warm potential cybercriminals, government has enacted the 'Digital Security Act, 2018'. This act deals with the new horizon of cybercrimes such offence related to the illegal entrance in critical information infrastructure, transmitting any information which is defamatory in nature, tampering with computer source documents, digital or electronic fraud, etc. But to remove any type of legal hurdles, the present legal instruments need to be analysed to test whether provisions are adequate to combat any cybercrime or not and to recommend necessary changes as needed.

2 Defining cybercrime

As the nature of the technology is progressive, it is hard to confine the term 'cybercrime' within the boundary of a concrete definition. Generally, cybercrime refers to all crimes using a computer or network (Moore, 2005) system where such computer or network system is a tool or target of the crime (Kruse and Heiser, 2002). Normally, it denotes to the harmful actions or omissions done by the use of computer or computer network (NCIS, 1999). Cybercrimes are those crimes committed in a network environment or on internet (Mia, 2015). It is also defined as: "offences that are committed against individuals or groups of individuals with a criminal motive causing harm to the victim physically or mentally using modern telecommunication networks (networks including chat rooms, emails, notice boards and groups) and mobile phones – Bluetooth/SMS/MMS" (Halder and Jaishankar, 2011).

Chick differentiates between the concept of computer crime and cybercrime:

a Committing crime using special knowledge of computer technology is called computer crime.

b On the other hand, where the offender uses special knowledge of cyberspace as means of committing a crime is cybercrime (Wai and Chick, 2007).

The absence of an appropriate and comprehensive definition of the phraseology leads to draw the following inclusiveness, e.g., cyber-trespass, cyber deception, cyber pornography and cyber violence (Sahoo, 2017).

3 Defining social media

The emerging interests of people worldwide and easy accessibility of the internet leads to the coining of the term 'social media' (Kaplan and Michael, 2010) which is yet to be defined constructively and exhaustively. Social media 'is interactive Web 2.0 internet-based application that facilitates the development of social networks online by connecting a profile with those of other individuals and/or groups' (Jonathan and Steve, 2015). Moreover, social media is a recent form of computer technology which facilitates to dispense the thinking, views, opinions, and information in the society through the medium of virtual networking system. SNSs permit people to build up their own profile under a sophisticated system and sort out the lists of their chosen one to share connections and views (Ellison, 2007). Technically, this system relies on the internet and supplies its users with a quick and easy method of sharing ideas and thoughts electronically. Social media users get themselves engaged by internet-based software and applications operated through computers or other electronic devices like smartphones, tabs, smartwatches, etc. SNSs are basically used for making and distribution of multiple social information, data, ideas, job vacancies and many other kinds of information people in need by computer networks. For its popularity and easy accessibility, now it has become a market place as the targeted customers can be reached out very easily here. It happens because the SNSs have enormous power of keeping almost every user connected together and sharing thoughts and ideas very swiftly worldwide.

Social media may contain a variety of activities based on a digital device as like photo sharing, writing, social gaming, social interaction, video transmitting with each other, commercial adds, reviews, etc. Even it is used nowadays as a strong tool of governance and motivating voters at the time of the election. But in personal life, social media is used to maintain personal communication with friends and family members, obtain career facilities, find people across the world of the same character and interests, and share their thoughts, feelings, and passions and those who involve themselves in these activities are called to be a part of virtual social network.

3.1 General concept of 'social media' and how does it affect our understanding of cybercrimes in Bangladesh

Social media refers to interactive computer-based technologies through which the spread of information, mutual interaction, sharing of opinions and diverge forms of communication can be executed with hardly any effort (Ahmed, 2009). The definition of social media therefore becomes formidable owing to their outstanding and established positions in the present world. However, here are some common features:

1 Social media are interactive Web 2.0 internet-based applications.

2 User-generated content such as text posts or comments, digital photos or videos, and data generated through all online interactions, is the lifeblood of social media. Users create service-specific profiles for the website or app that are designed and maintained by the social media organisation.

3 Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups.

Though the various features and service make it difficult to provide an exclusive definition of the social media, the concerned marketing and social media professionals broadly agree that social media embodies the following 13 types:

- blogs
- business networks
- collaborative projects
- enterprise social networks
- forums
- microblogs
- photo sharing
- products/services review
- social bookmarking
- social gaming
- social networks
- video sharing and
- virtual worlds.

By the passages of time, technology has brought a revolutionary change in the life of people. The modern communication system is one of the blessings of contemporary technology. People in this 21st century are using a variety of platforms and media to communicate with others. Among them, social media is one of the latest additions to this run of invention of technology. Social media is rapidly evolving and becoming a very important part of everyday life for the advancement of technology. The increasing use of smartphones has also contributed a lot to the enchantment of social media widely. At present, it has been so popular that people of all classes and ages use it as an important media of communication. Among the various types of social media, blog, Facebook, Twitter/Flicker are prominent (Alam, 2007). In Bangladesh, the use of the social media platforms has also been increasing rapidly over the last few years. People who have internet access have one or more accounts at one or several social media platforms, i.e., Facebook and Twitter. The enormous use of social media is both directly and indirectly affecting the way of communication as well as the life of the people.

As computers, smartphones and internet connection is directly connected with the use of social media, the incidents of cybercrime is also increasing rapidly in Bangladesh. At present, about half of its total population, especially the young generation aged six to 25, is connected with different platforms of social media (Firoz, 2016). A recent survey reveals Dhaka, the capital city of Bangladesh, as the second highest number of Facebook users in the world. Though different countries in the world have taken this as an alarming issue and have passed special laws regulating cybercrime through social media, Bangladesh is yet to mention the term in its two legislations, the latest one passed in 2018.

As crimes can be committed from any remote location, for example, any country, most criminals choose cybercrime because they are less likely to be caught and punished (Taylor, 2006). Therefore, the unbound and over increasing incidents of cybercrime in social media, mostly targeting the women, children and teenagers, and the vast presence of uncontrolled content, which is not only illegal but also harmful, has left the authority concerned in dire need of regulating a 'new' law. The existing laws and its legislations in Bangladesh are vast but they theoretically do not cover issues relating to social media due to the unavailability of appropriate provisions in relative sectors (Khan, 2018). The recent emergence of online activity due to Covid-19, especially the over increasing online fraud using social media has strengthened the need for regulating the social media activities through a separate but special law.

3.2 How does it dispute or alter our definition or conceptualisation of social media? A wider context for the case of Bangladesh

Social media has outstandingly been playing a vital role in conflict and contentious politics over the years. People of all walks of life including politicians, leaders, insurgents, and protestors use it as a tool for communication. Besides, the researchers and scholars have also turned to social media as a source of new data on conflict. The following framework given will help us to understand the influence of social media through four interplead points:

1 social media lowers the costs of communication

2 it enhances the speed and dissemination of information

3 scholars should focus on the strategic interaction and competitive adaption of actors in response to communication technology changes

4 the new data that social media provides are not only an important resource, but also fundamentally change the information available to conflict actors, thereby shaping the conflict itself.

However, social media's influence on conflict defies simplistic explanations that argue that it privileges incumbents or challengers.

There is no way to deny that SNS is one of the greatest innovations of modern times. Among various types of SNS, Facebook and Twitter are most popular all over the world (Bleyder, 2012). People of Bangladesh mainly use Facebook for social communication, online shopping, business, knowledge and experience sharing, etc. However, individuals are often engaged in real life violence, caused by certain posts or events in social media (Hasib, 2009). The table given will provide some examples of the real life violence originated from Facebook activities in Bangladesh. In these cases, Facebook was used intentionally or unintentionally as a tool to trigger hatred and violence. In this study, the authors briefly discuss (on the basis of case study) five notable and devastating incidents, triggered by Facebook activities.

Table 1 Examples of the real-life violence originated from Facebook activities in Bangladesh

Number	*Year*	*Location*	*Triggered by*
1	2012	Ramu	Post image on Facebook
2	2013	Pabna	Facebook post
3	2014	Cumilla	Comment on a Facebook post
4	2016	Brahmanbaria	Facebook post
5	2017	Rangpur	Facebook post

Source: Authors survey

One of the devastating incidents originated from Facebook activities in Bangladesh was 2012 Ramu Violence. In the late September in 2012, the monasteries, shrines, and houses of Buddhist inhabitants were burnt to the ground following an image posted on Facebook wall that depicted the desecration of a Quran (the central religious text of Islam, believed by Muslims to be a revelation from God). The image was posted on the Facebook wall of Uttam Kumar Barua, a local Buddhist, by an unknown or fake user using a pseudonym. Following the Facebook post, thousands of people brought out protest processions and eventually vandalised and put fire on the temples, shrine, monasteries and houses of the Buddhist claiming that Buddhist youth Uttam Kumar Barua 'insulted Islam' on social media. Later, it was found in the several media and government reports that the Buddhist Uttam Kumar Barua was innocent and it was provoked by someone intentionally. The Ramu Violence clearly depicts how social media was used then to reach a vast number of people within a very short time. It was evident that nobody then raised any question about the authenticity of the Facebook post while a group took the advantage of social media.

A year later, violence ensued following a fake Facebook post at a Hindu dominated neighbourhood in Bonogram area of Pabna district in Bangladesh on November 3, 2013. Several mobs went on rampage and vandalised several idols and temples, and 25 houses of Hindu community following a Facebook post, reportedly posted by the minority boy Rajhib Saha on a 'Facebook page' that maligned Prophet Muhammad (pbuh). About 150

Hindu community families had to flee the area to save them from the attack. However, it was reported later that the boy had no connection with the Facebook page or post. Rather, he was framed by someone intentionally misusing Facebook.

In Comilla district of Bangladesh, another attack was carried out on the Hindu community at Bakhsitarampur village under Homna upazila in 2014 following a rumour based on Facebook that left at least 28 houses of the community ransacked. Around 3,000 protesters went on rouge on the neighbourhood Hindu community after news that two Hindus posted defamatory comments on Facbeook about Prophet Muhammad (pbuh) disseminated online that happened to be fake. Social media had also been used to trigger violence in this incident.

The following year, 2016, marks another devastating violence originated from a Facebook post at Nasirnagar upazila in Brahmanbaria district in Bangladesh. Series of attacks was carried out and at least 15 temples and 150 houses of the Hindu community people were vandalised, looted, and set on fire after a Hindu fisherman reportedly mocked a holy site in Mecca on Facebook. At least hundred people including several devotees received injuries in the attacks. Later, the police found that it was not the fisherman who mocked the holy site. Rather, it was another person who opened an account with the name and picture of the fisherman and mocked the holy site to take revenge on him.

On 10 November in 2017, a mob went rampage again on the Hindu community people at Thakurpara village in Rangpur in Bangladesh following another Facebook post hurting religious sentiments of the local people. Reacted by this alleged 'Anti-Islam' Facebook post, the agitating mob vandalised and burned at least 30 houses of the Hindu community people to ashes. The violence left one person killed and about 20 others injured as the local police fired rubber bullets and teargas shells to bring the situation under control. Later, it was revealed in an investigation report of police that the Facebook account was hacked and the person, who hacked the Facebook account, did it intentionally. So, it was evident that misuse of Facebook has been continuing since its widespread use in Bangladesh.

3.3 A brief comparison with neighbouring country with social media and cybercrime issue

The emergence of IT has enabled people to interact and convey their feelings and ideas in an expedited manner in India which shares its border with Bangladesh. The number of social media users in India, especially the young generation, has been on the rise as it ensures the freedom of speech and expression (Big Commerce, 2020). It allows people of all walks of life including those who are marginalised to raise their voices and opinions freely. Along with the overlapping users, the incidents of revenge porn, cyberstalking and slut shaming have also been increasing in social media platforms over the years. To address these vast numbers of crimes, social media platforms' crowd reporting mechanism has already been proved to be largely inefficient. However, these incidents or crimes are not being subjected to serious debates and discussions though they crimes are increasing sharply. Each day, a number of cases are being reported but they are many times fewer than the actual number of crimes happening on social media platforms. Even cyber-aggressions are not viewed often as crimes. In 2017, more than 300 cases of cybercrime related to social media were reported in 2017. The number was double than

that of the previous year. In 2016, there were only 150 cases reported in the country (Statista, 2020).

In India, the rights of expressing free political views about religious activities of women are reserved under Section 295 A of the Indian Penal Code (Indian Penal Code, 1860). However, the hard-core devotees who assert themselves as the protectors of the religious faith and deities subject those women to verbal abuse without being touched by the so-called secular laws. The legal framework also shamefully normalises the execution of women belonging to opposition parties and who raise their voices of dissent against established religious institutions. And, these violent incidents even cannot get its way to discussions on social media platforms. Abuse on SNSs is usually being addressed under the criminal laws that deal with conventional offences such as sexual harassment, privacy infringement, criminal intimidation and defamation. These give off an impression of being to a great extent deficient to deal with the techno-motivated offences, which have a more profound, ruthless effect on the victim than these traditional crimes. The sole cause for this inefficiency is the rejection of the legislators to guarantee secure virtual social platforms for their woman voters. The helplessness of women in social media platforms resulting in their exit or forced silence on social media apprehending personal violence, victimisation and stigmatisation does not add any merit to the country's criminal justice system (Amnesty International India, 2020) but exasperates disfavour to its disappointments and entanglements.

4 Most popular social networking apps in Bangladesh

The network service providing companies have already launched numerous social networking apps that are used in maintaining internet-based communication with each other. But all of them could not get the same popularity among the users. However, the rate of using any social networking apps may vary from country to country. The trends of using social media among Bangladeshi people of all ages are increasing day by day particularly among the young generations where 73% users are aged between 13–25 (Shams, 2017). The popular social media networking sites available in Bangladesh are Facebook, Twitter, YouTube, WhatsApp, Google+, LinkedIn, Instagram, Pinterest, Imo, Skype, Ovizan, and so on. Among these, Facebook is the most popular one where users are around 35,853,000 (napoleoncat.com) IMO and WhatsApp are not behind in popularity as nowadays people from almost all classes use them as an alternative to direct phone call and LinkedIn is popular to the professionals.

Moreover, the sum of the population of Bangladesh is approximately 166.5 million whereas 36% of them are living in the cities. Almost 99.428 million people of the country use internet and approximately 36 million of them are active in different social media, mostly in Facebook and it was estimated that 96.94% users of social media use Facebook which has become the most significant sector for social media and digital marketing in the country. On the other hand, about 137.2 million people are using mobile phones and 76.22 million are active on internet by using mobile phones. Among the users of social media, 74% was identified as male where only 26% from female and about 28 million of them which is the amount to 17% of social media users are active in social networks by their cell phones. Besides that, from January 2017, there has been shown an increase in the users of internet that amounts to 27% while it is 15% in social media (Jain, 2018).

5 Type of crimes frequently happening in social media of Bangladesh

Generally, computer crime or cybercrime includes a very wide range of activities happening through electronic devices (Gordon and Ford, 2006). Here are some examples of those as frequently occurred throughout the world.

5.1 Cyber fraud in social media

People are more interested or somehow bound as the demand of the system to share their personal details, e.g., birthday, contact address, e-mail, hometown, relationship status on their social networking profiles. Nowadays, social media has been the best place for investors worldwide to advertise them, to gather information or to sell their products but its number of features also poses a threat by attracting fraudsters for the crime. Phishing is also considered as technical fraud by social engineering where huge emails are sent to secure the trust of the targeted victim and asking him to do as directed rather rationally. Instead of adequate measures are taken for security, the criminogenic aptitudes of potential cybercriminal has given way to new kinds of crimes like cyber fraud which includes selling and buying of stolen goods, non-delivery of products or services, payment fraud, online advertising frauds and the most familiar one is opening fake IDs on SNSs.

The number of cybercrimes has mushroomed in Bangladesh in the last few years as the cases increased to 925 in 2018 from only three in 2013 (Tipu, 2019). A report recently published by Cyber Crime Awareness Foundation (CCAF), also revealed that around 73.71% of victims (both male and female) are aged between 18 and 30 years, 10.52% are below 18 while 12.77% between 30–45 years and 3% above 45 years of age.

5.2 Online sexual extortion

The 'intrusion into one's personal or familial affairs by physical means or publication of information' (Calcutt, 1993), has a profound link with unexpected enlargement of different methods of communication. Sexual extortion – a serious crime where a perpetrator threatens to publish the victims' private and sensitive material online unless they hand over money and has become very common phenomenon' (Kopecký et al., 2015) and teenagers are the most vulnerable cyber-victim of Almost in all cases, it seems to be committed by boys or men against girls (UNICEF Study Report, 2016) and relatively a very small number of online child abuse cases are reported or caught (Açar, 2016). Recently in Bangladesh only two victims sought help from police by calling 999 (national emergency helpline) and all efforts taken were unsuccessful and of which 70% of cybercrime victims are women and children between 15–25 years of age, and ironically most of the perpetrators are young men between 17–25 years (Rob, 2019).

5.3 Online threats and stalking on social media

Another form of cybercrime social media users facing is cyber threats or stalking others through online. Most users (one out of every 12 women and one out of every 45 men in the USA and every 14 people out of 1,000 at their 18 age) become an easy prey of privacy invasion because of the difference of the information disclosed, underestimating

the authentication system and non-understanding of privacy preferences. One Americans out of ten has suffered from online harassment and about 7% have suffered from cyberstalking. If such offenses go unpunished regularly, victims would think it normal misbehaviour making room for offenders for further and more severe form cyber criminality.

5.4 Hacking of social media accounts

Of all types of online offences, hacking (an act of unlawful intrusion into a computer or network system protected and secured by another person without his permission) is very common. It means an 'unauthorised access and subsequent use of other people's computer system' (Hacker, 2006) and unlawful intrusion into a computer system for obtaining confidential information (Ahmed et al., 2017) which subsequently is used as means of financial extortion. Criminals stealing emails and passwords send requests for financial assistance from social media friends of the user who's the account is hacked by false personification (Rahman and Mumtaz, 2019). In Bangladesh report of The Cyber Safety Program Wing of the ICT Ministry revealed that among over 2,000 complaints filed in January and February of 2016, incidents of Facebook ID hacking were more than 1,200 and in 2015–2016, the total number of complaints was around 8,000 (Khan, 2016). Recently, Dhaka Metropolitan Police (DMP) arrested an accused for hacking 200 Facebook IDs and demanding money or threatening people for spreading obscenity in their IDs.

5.5 Spreading malware and viruses through social media

The very recent form of cybercrime happening in different social media is spreading viruses and malware through SNSs. Cybercriminals developing malware and harmful computer programs ambush them in various links and attachments and whenever the user responds to them, it infects their computer. According to a survey, around 70% companies were anxious for their network security as their employees use social media and approximately, 40% social media users are the victim of virus infection (NW3C Report, 2011).

Table 2 Examples of some occurrences

Number	*Year*	*Location*	*Triggered by*
1	2012	Ramu	Posting image on Facebook
2	2013	Pabna	Facebook post
3	2014	Comilla	Comment on a Facebook post
4	2016	Brahmmanbaria	Facebook post
5	2017	Rangpur	Facebook post
6	2019	Bhola	Facebook post

Source: Authors survey

5.6 Fabricating news on social media

Cybercriminals often use social media to make community disorder. They post on Facebook, Twitter, WhatsApp, etc. something having no reality (Dashora, 2011). It is generally about the religious matters which results in the breakdown of the non-communal harmony in the country. Bangladesh has already got a number of awful experiences of the communal disorder between different religious groups of the country.

5.7 Posting videos of criminal activity

Very recently posting of videos of criminal activity by the criminals becomes a common phenomenon as a heroic symbolisation of their criminality or as an open threat to the victims. Most of the victims are blackmailed by threatening to post those videos and making it viral on social media. On 15th January 2020, four rapists from Kishorgonj district of Bangladesh appeared on Facebook live joyfully, after committing the offence. Though it is horrifying, police and prosecutors can trace the offenders as well through digging its source as it happened in Kishorgonj incident.

5.8 Bullying on social media

It is very common feature in Bangladesh that users thereof often comment or share various posts made by others without justifying. As a result, it often acts as a catalyst in breaching the peace of society. For example, in July 2019, a rumour had been spread by a Facebook post that heads of the human being need for continuing the construction and it resulted in deaths of a number of people by public beating on the suspect of the kidnapper. Finally, the authority of the construction issued notification for public awareness.

6 Data analysis of cybercrimes in social media of Comilla district, Bangladesh (2018–2019)

The police report of 17 police stations located in Cumilla shows that sixty-two cases were filed under the ICT Act, 2006, Pornography Control Act, 2012 and the Digital Security Act, 2018 for the last 22 months. In 2018, 18 cases accusing 40 persons were filed under the ICT Act, 2006 where no case was filed under the same act from January to October 2019. Fourteen cases were recorded under the Pornography Control Act, 2012, in 2018 where a sum forty people were accused therefore, but only 17 of them were arrested. The cases under the same act increased twice in 2019 from January to October. Eight cases under the Digital Security Act, 2018, were filed in the last three months in 2018 after it being enforced which is two times higher than the previous eight in ten months in 2019.

It is vibrant from above two charts that number of cases under the ICT Act, 2006 is decreasing as there is no case in 2019 under the same act. The Digital Security Act, 2018 covers all cases used to deal with the ICT Act, 2006. However, cases under Pornography Control Act, 2012, possess the large portion in the two charts and they are increasing as eighteen cases have already been filed in ten months in 2019 while it was 14 in total in 2018. In this area, women are in a vulnerable position as their husband threatens to

publish their personal videos as made by themselves. It was clear while the survey was going on as two cases namely, *Ayesha Akter vs. Hossain* and *Sayema Mojumder vs. Tipu Sultan*, are bearing the same fact that both victims filed cases against their husband complaining that he posted her porn made him while they enjoying matrimonial rights.

Figure 1 Shows the number of cases related to the cybercrime in Cumilla in 2018 (see online version for colours)

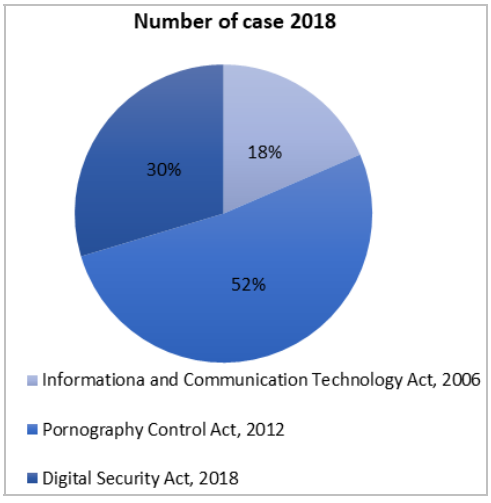
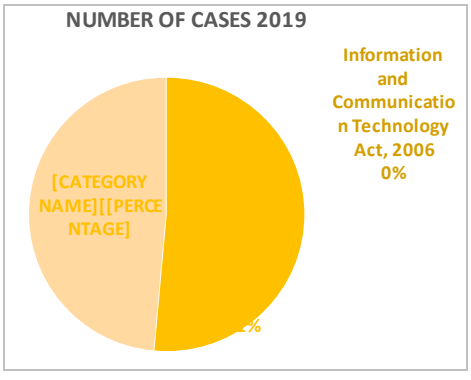


Figure 2 Shows the number of cases related to the cybercrime in Cumilla in 2019 (January to October) (see online version for colours)



7 Legal frameworks related to controlling the cybercrimes on social media in Bangladesh

Bangladesh is now marching fast towards development especially in IT sectors. As its part of the development scheme, the Government has launched 'Bangabandhu Satellite' on May 11, 2018, possessing control over space and has started thinking of launching 5G network.

Every invention has two aspects, both good and bad. People with a guilty mind use the technology to commit various crimes which are different from general crime as defined in the Penal Code, 1860. Thus, the Government of Bangladesh has already made several laws to regulate the activities of its subjects in the cyber-space and to punish the criminal of the sector.

However, as to the trial procedure, the Code of Criminal Procedure, 1898, shall be followed in adjudicating the cases under the purview of the computer-related crime.

7.1 The ICT Act, 2006

Undoubtedly The ICT Act, 2006 was a fabulous stage especially when there was no regulation on this particular field. Technology has been grossly misused from the last decades, which demands statutory laws to control those criminal activities and to give redress to the victim. To accelerate this purpose, The ICT Act, 2006 has been passed and amended by an Ordinance on 20 August 2013.

Under this Act, any person who secures access or attempts to secure access to a protected system in contraventions of sections 47 of the Act, then this activity would be regarded as an offence for which the punishment may extend to 14 years imprisonment or fine of 10 lakhs taka or both (The ICT Act, 2006).

The Act also provides that any person who has secured access to any electronic record, book, register, correspondence, information, document or other material and without the consent of the person concerned, discloses such record, book, register, correspondence, information, document or other material to any other person shall be regarded as an offence which is punishable with imprisonment for a term which may extend to 2 years, or with fine which may extend to 2 lakhs taka, or with both (Section 63 of the ICT Act). The Act further provides that whoever knowingly assists committing crimes under this Act, using any computer, e-mail or a computer network, resource or system shall be regarded as an offence and punishable as the core offences (The ICT Act, 2006).

After amendment of the act repealing sections 54, 55, 56, and 57, the Act is now in a handicapped mood having no active role in controlling cybercrimes both in general and social media sectors. Nevertheless, the sections discussed above are to some extent relevant, though not sufficient, in controlling offences committing using social media.

7.2 The Digital Security Act, 2018

Basically the Digital Security Act, 2018, is a modification of the ICT Act, 2006. Some sections such as 54–57 of the ICT Act, 2006 were repealed by the Digital Security Act, 2018; the provisions of those sections were substituted in the later act with a modified face. To combat unaccepted restrictions lying under different sections of the ICT Act, the government enacted new digital security act, 2018.

The Digital Security Act is to replace the much-criticised ICT Act and to combat cybercrime. Now the question arises as to how far it is effective. Does it strike a blow to freedom of speech in the country or a threat to freedom of expression in social media or can we predict that this act will be an operative utensil to combat any type of cybercrime both in present and future? This act has drawn serious concerns for imposing restriction on exercising our rights but at the same time, it has widened its scope to cover different

types of cybercrime as today when we find people of different ages active in social media. Analysis of important provision will help us to understand the impact of the act.

This act enumerates punishment for any propaganda or campaign against liberation war, cognition of liberation war, father of the nation, national anthem or national flag. No doubt this provision covers a wide area nevertheless, the Act authorises sentences of up to 14 years in prison for all of the facts stated above of which punishment for the expression of opinions about historical facts are incompatible with a country's obligations to respect freedom of opinion and expression.

This Act delineates punishment for Publishing, sending of offensive, false or fear-inducing data-information, in any website or through any digital medium or propagating or assisting in publishing or propagating any information with the intention of tarnishing the image of the nation or spread confusion or despite knowing it as false. This definitely warns people who are publishing or sending any content intentionally or knowingly but the vagueness, combined with the harsh potential penalty and increases the likelihood of self-censorship. Under this Act, "broadcast, etc. of such information in any website or in any electronic format that hampers the religious sentiment or values" is an offense punishable with imprisonment not exceeding five years or fine not exceeding 10 lac or both.

Besides it provides an outline where a person will be sentenced to a term of imprisonment not exceeding three years or fine not exceeding Tk. 5 lac or both If he commits an offence of publication or broadcast defamatory information as described in section 499 of the Penal Code in any website or in any other electronic format. Sections 28, 29 along with 31 grants law enforcement authorities wide-ranging powers to remove or block online information that "harms the unity of the country or any part of it, economic activities, security, defence, religious value or public order or spreads communal hostility and hatred" and to conduct warrantless searches and seizures if a police officer has reason to believe it is possible that 'any offense under the act' has been or is being committed. If law enforcing authorities are aware of their respective power but not to abuse it then obviously it will be a tool to protect and respect the fundamental rights of every citizen enshrined under article 39 of the constitution of Bangladesh and to fulfil the international obligation of the government of Bangladesh and to bring to book the offender without unnecessary delay.

7.3 The Pornography Control Act, 2012

The Pornography Control Act, 2012, has been enacted to prevent the deterioration of ethical and social values as pornography destroys moral values in the society and causes various offences resulting in disorder in the community. The Act says that production, preservation, carrying, the supply of pornography cannot be done. According to the same section, selling, buying, making, or displaying of pornography is illegal and punishable offence even if it be on social media.

Various social media available in Bangladesh like *Facebook*, *Imo*, *WhatsApp*, *Viber*, *Snapchat* are being used as tempting instruments to transmit online materials, e.g., video clips, pictures, voice recordings, etc. from part of the globe to another. Under this Act, distribution, publication and dissemination of all those materials in any form, both printed and electronic, constitute an offence. Even though some people think that the videos recorded or pictures taken or voice recorded with the consent of the victim would not

form it as an offence under the Act, but Section 8 delineates it as an offence and the offender would be punished for the imprisonment of seven years.

The Act has also provided a section for child pornography and any pornography recording, pictures and filming anything punishable under this Act of a child below the age of 18 years would be punishable with imprisonment of ten years and fine of 5 lac takas. Under this Act, the court is empowered to take expert opinion from IT experts and investigating officer (IO) is also authorised to search and seize any electronic devices, documents and other relevant online materials as evidence. The Act further enumerates that with a view to accelerating the speedy disposal of cases under the Act, the government may establish a separate tribunal which is not established yet. Any person convicted with false and frivolous allegation shall be sentenced for two years' imprisonment and fine up to 1 lac taka.

If any person files a false or vexatious case against a person under this act with a view to causing damage to him mentally or physically or economically or it is proved that the case was vexatious, the concerned person shall be sentenced with rigorous imprisonment not exceeding two years and fine up to 1 lac taka. Though this act was passed with a great motive to control the rapidly increasing number of sexual and obscene activities in online including different social media nevertheless it has failed to achieve it. A very few cases have been filed under this Act so far and the dismissal rate is not satisfactory as well. Most of the victims are completely unaware of the legislation.

8 Recommendations to prevent cybercrime in social media of Bangladesh

Prevention is always the best solution than cure. A social media user must be careful and cautious while operating various social media sites by posting videos, audios, comments, references of other news or posts, and transmitting messages. Any type of negligence may make his/her social media life complicated with severe consequences in real life. A social media user and the state should keep in mind the following instructions for the prevention of social media harassment:

1 To avoid disclosing any personal information pertaining to oneself in SNSs.

2 To avoid sharing any photographs, videos, images using social media apps to unknowns and even to friends as it may be misused over time.

3 To monitor and observe closely the SNSs visited, apps used, online social communities integrated and links attached by the children is important by the parents to protect them from online harassment.

4 Revising and restructuring existing legal frameworks befitting with the demands of the cyber world.

5 Using strong passwords or other security processes for different social media sites following the directions of the sites.

6 Different social awareness programs should be launched to make the young users cautious of the various threats in social media use and their speedy recovery systems.

7 As often every student both undergraduate and graduate level is now connected to the use of social media sites, a book chapter can be included in the ICT course on social media use discussing the threats and precautionary steps.

8 Law enforcing agencies should be equipped with sophisticated technological instruments and be trained to cop up with the advancing rate of cybercrimes in social media.

9 Government bodies like BTRC should be aware of the users having details and must have a coordinating mechanism with owners of the social networks to find out the criminals easily.

9 Conclusions

Human life was effortful before the wonderful invention of modern science. As the internet made our daily-activities easier, it also facilitated ways to do its related crimes for the criminals. Cybercriminals availing of unawareness and inefficiency of the human beings in using the internet do various crimes which compel the authority of the states to thinks of the ways to prevent them. A constructive solution is taken for children. The most recent optional protocol to the CRC, the OP3 on a communications procedure, allows minors to file a direct complaint to the UN, when their national legal system cannot guarantee remedy. Cybercrime causes huge damage in the world economy. In August of 2016, cybersecurity ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. So, it is our common duty to be more conscious while we use the internet especially social media sites and other modern technology.

References

Açar, K.V. (2016) 'Sexual extortion of children in cyberspace', *International Journal of Cyber Criminology*, DOI: 10.110-126.10.5281/zenodo.163398.

Ahmed, S., Kabir, A., Sneha, S.S.A. and Jafrin, S. (2017) 'Cyber-crimes against womenfolk on social networks: Bangladesh context', *International Journal of Computer Applications*, Vol. 174, No. 4, pp.9–15.

Ahmed, Z. (2009) *A Textbook on Cyber Law in Bangladesh*, p.56, National Law Book Company, Dhaka.

Alam, M.S. (2007) 'Cyber-crime: a new challenge for law enforcers', *Journal of University of Information Technology and Sciences*, Vol. 2, No. 1, pp.25–32.

Amnesty International India (2020) *How to Protect Yourself from Online Violence: A Guide For Women in India* [online] https://amnesty.org.in/how-to-protect-yourself-from-online-violence-a-guide-for-women-in-india/ (accessed 13 October 2020).

Big Commerce (2020) *Know to Social Media Now* [online] https://www.bigcommerce.com/blog/social-media-advertising/#what-are-the-benefits-of-advertising-on-social-media-channels (accessed 6 October 2020).

Bleyder, K. (2012) *Cyber Security: The Emerging Threat Landscape*, pp.52–53, Bangladesh Institute of Peace and Security Studies, Dhaka.

Calcutt, S.D. (1993) *Report of the Committee on Privacy and Related Matters* [online] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/271963/2135.pdf (accessed 20 June 2020).

Dashora, K. (2011) 'Cyber crime in the society: problems and preventions', *Journal of Alternative Perspectives in the Social Scien*ces, Vol. 3, No. 1, pp.240–259.

Ellison, N.B. (2007) 'Social network sites: definition, history, and scholarship', *Journal of Computer-Mediated Communication*, Vol. 13, No. 1, pp.210–230.

Firoz, A. (2016) 'Present internet users and websites in Bangladesh', *The Daily Star*, 13 June 2016 [online] https://www.thedailystar.net/business/present-internet-users-and-websites-in-bangladesh-2336477 (accessed 20 September 2020).

Gordon, S. and Ford, R. (2006) 'On the definition and classification of cybercrime', *Journal in Computer Virology*, Vol. 2, No. 1, pp.13–20.

Halder, D. and Jaishankar, K. (2011) *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*, p.11, IGI Global, Hershey.

Hasib, A.A. (2009) 'Threats of online social networks', *International Journal of Computer Science and Network*, Vol. 9, No. 11, pp.288–293.

Indian Penal Code (1860) [online] https://www.indiacode.nic.in/handle/123456789/2263?locale=en (accessed 9 October 2020).

Jain, S. (2018) *30 Bangladesh's Digital Marketing and Social Media Marketing Stats and Facts* [online] https://www.soravjain.com/digital-marketing-and-social-media-marketing-stats-and-facts-of-bangladesh (accessed 12 July 2020).

Jonathan, O. and Steve, W. (2015) 'Social media definition and the governance challenge: an introduction to the special issue', *Telecommunications Policy*, Vol. 39, No. 9, pp.745–750.

Kaplan, A.M. and Michael, H. (2010) 'Users of the world, unite! The challenges and opportunities of social media', *Business Horizons*, Vol. 53, No. 1, pp.59–68.

Karzon, S.H.R. (2008) *Theoretical and Applied Criminology*, p.56, Palal Prokashoni, Dhaka.

Khan, J. (2018) 'Two arrested over fake news sites', *The Daily Star*, 30 November 2018 [online] https://www.thedailystar.net/city/creating-fake-prothom-alo-news-website-2-held-in-dhaka-1666777 (accessed 17 October 2020).

Khan, M.J. (2016) 'Hackers robbing Facebook users', *The Daily Dhaka Tribune* [online] https://www.dhakatribune.com/uncategorized/2016/02/28/hackers-robbing-facebook-users (accessed 20 March 2020).

Kopecký, K., Hejsek, L., Kusá, J., Marešová, H., and Řeřichová, V. (2015) *2nd International Multidisciplinary Scientific Conference on Social Sciences and Arts SGEM2015* [online] https://istina.msu.ru/conferences/10910584 (accessed 10 August 2020).

Kruse, W.G. and Heiser, J.G. (2002) *Computer Forensics: Incident Response Essentials*, p.392, Addison-Wesley Professional, Boston.

Mia, B. (2015) 'Cybercrime and its impacts in Bangladesh: a quest for necessary legislation', *International Journal of Law and Legal Jurisprudence Studies*, Vol. 2, No. 4, pp.1–18.

Moore, R. (2005) *Cyber-Crime: Investigating High-Technology Computer Crime*, p.25, Anderson Publishing, Mississippi.

Nahar, J. and Minar, M.R. (2018) 'Impact of social media post in real life violence: a case study in Bangladesh', *Arson and Violence in Bangladesh Triggered from Social Networks Project* [online] https://www.researchgate.net/publication/329783323_Impact_of_Social_Media_Posts_in_Real_life_Violence_A_Case_Study_in_Bangladesh (accessed 10 May 2019).

National Criminal Intelligence Service (NCIS) (1999) [online] https://www.file:///C:/Users/ASUS/Desktop/Insight_to_Cybercrime.pdf (accessed 22 February 2019).

NW3C Report (2011) *Criminal Use of Social Media* [online] https://www.nationalpublicsafetypartnership.org/clearinghouse/Content/ResourceDocuments/Criminal%20Use%20of%20Social%20Media.pdf (accessed 12 March 2019).

Rahman, S.T. and Mumtaz, H. (xxxx) 'Social media-related cybercrimes and techniques for their prevention', *Applied Computer System*, Vol. 24, No. 1, pp.9–17.

Rob, R. (2019) 'Online sexual extortion: why we can't protect the most vulnerable?', *The Daily Star* online] https://www.thedailystar.net/opinion/news/why-cant-we-protect-the-most-vulnerable-1779211 (accessed 20 May 2020).

Sahoo, G.P. (2017) *New Legal Dimension of Cyber Crime*, p.416, Satyam Law International, New Delhi.

Shams, S.R. (2017) 'Social media trends usages in Bangladesh', *The Daily Asian Age*, 2 February 2017 [online] https://dailyasianage.com/news/46958/social-media-trends-usages-in-bangladesh (accessed 20 June 2020).

Statista (2020) *Cybercrime in India-Statistics and Facts* [online] https://www.statista.com/topics/5054/cyber-crime-in-india/ (accessed 13 October 2020).

Taylor, P. (2006) *Hacker: Crime in the Digital Sublime*, p.22, Routledge, London.

The ICT Act (2006) *Act No. 39 of 2006, Amended in 2013* [online] http://www.icnl.org/research/library/files/Bangladesh/comm2006.pdf (accessed 18 March 2019).

Tipu, M.S.I. (2019) 'Over 900 cases related to cybercrimes filed in 2018', *The Dhaka Tribune*, 21 April 2019 [online] https://www.dhakatribune.com/cybersecurity/2019/04/21/over-900-cases-related-to-cybercrimes-filed-in-2018 (accessed 14 January 2020).

Ullah, H.S. (2019) *Social Media and its impact on Bangladesh* [online] https://www.academia.edu/12318661/Social_Media_and_its_impact_on_bangladesh (accessed 12 December 2019).

UNICEF Report (2016) *Victims are Not Virtual: Situation Assessment of Online Child Sexual Exploitation in South Asia* [online] https://www.unicef.org/rosa/reports/victims-are-not-virtual (accessed 15 August 2020).

Wai, K. and Chik, W.B. (2007) *Challenges to Criminal Law Making in the New Global Information Society*, p.348, Singapore Management University, Singapore.