Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context

Md. Abu Bakar Siddik[1]
Saida Talukder Rahi[2]

Abstract

With the arrival of Information Communication and Technology, the world has now become a digital world and the advent of this technology has made communication and economic transactions easier. Bangladesh is also introducing herself with this digital world and interestingly the present Bangladesh is called nationwide 'Digital Bangladesh'. But in this Digital Bangladesh, participation in social media especially in Facebook has increased melodramatically over the recent past years. The problem arises when the users of social media commit cybercrimes besides using this only as a tool of communication. When the people of Bangladesh are not widely known with internet and communication technology, in 2001 the Government enacted Bangladesh Telecommunication Regulation Act. Meantime the use of internet and social media increased and accordingly in 2006 the government enacted the Information and Communication Technology Act to prevent the possible cybercrimes. But this legislation was not enough to combat with increasing cybercrimes committed by offenders. As such the government in 2018 enacted another piece of legislation namely the Digital Security Act. But to combat cybercrimes in social media especially in Facebook how much effective is this Digital Security Act and ICT Act is a great concern. Hence this paper tries to analyse the existing laws and bodies regulating cybercrime in Bangladesh. The Paper reveals that the legal framework regulating cybercrime in Bangladesh is wide but technically hazardous and complicated. As such the paper dissects the provisions of existing laws largely ICT Act and Digital Security Act. The paper finally concludes by proposing Safety of Social Media and Misuse Restraint Act.

Keywords: Cybercrime, Social Media, Legal Framework, Bangladesh, Safety of Social Media and Misuse Restraint Act.

[1] The Author is a Lecturer at Department of Law of Comilla University, Bangladesh. He completed his LL.B. (Hon's) and LL.M. from the University of Chittagong, Bangladesh. His email address is absmasum.cu09@gmail.com

[2] The Author is a Lecturer at Department of Law of Comilla University, Bangladesh. She completed her LL.B. (Hon's) and LL.M. from the University of Chittagong, Bangladesh. Her email address is saidatalukderrahi@gmail.com

1.0 Introduction

At present often every internet user uses social networking sites and as such these sites have become a common platform of communication for these users. With the arrival of Information Communication and Technology (ICT), the world has now become a digital world and the advent of this technology has made communication and economic transactions easier. Anyhow the advantages, the development of the internet and the widened access to computer technology has not only granted new opportunities for easier communication, but has also created opportunities for those involved in illegal activities. The connection between organized crimes and the internet has increased the insecurity of the digital world. Thus, legislatures have been struggling to redefine laws that fit crimes committed by cyber criminals.

In 2001 Bangladesh enacted Telecommunication Regulation Act to stop any sort of unintended cyber incidents with the use of telecommunication tools. At that time no social media was invented and came to light and hence the Act does not think about cybercrime through social media but it had provision that cybercrime through internet via telecommunication medium would be punished under the law.

Bangladesh muscularly responded to cybercrimes in early 2006 by enacting the Information and Communication Technology Act (hereafter referred to simply as the 'ICT Act 2006'). The Act provides law enforcing agencies to investigate an offence and bring the offender to book under Cyber Tribunal. In 2013, the Government of Bangladesh introduced an amendment to the said ICT Act of 2006 that changed the complexion of criminal prosecution for online offences under the Act. In the following year the ICT Division has formed the Information Security Guidelines 2014 and the National Cyber Security Strategy of Bangladesh 2014 (hereafter referred to simply as the 'NCSS 2014'). NCSS addresses only the country's national security strategy and its purpose is to create a coherent vision for 2021 keeping Bangladesh secure and prosperous by coordinating government, private sector, citizens and international cyberspace defense efforts. But with the continuity of time and rapid evolution of cybercrimes, the ICT Act and NCSS turned out to be inadequate. In the meantime social media conquered the mind of mass people and its use became higher day by day. As such to combat the unprecedented cybercrimes committed by using internet, the government has enacted the Digital Security Act 2018.

The Digital Security Act deals with new horizon of cybercrimes such as offence related to illegal entrance in Critical Information Infrastructure,

transmitting any information which is defamatory in nature, tampering with computer source documents, digital or electronic fraud etc. The Act provides punishment for posting offensive content, cyber-terrorism and defamation, etc via internet amongst others but it does not contain any special provision relating to cybercrime through social media. As such to remove any type of legal hurdles, the present legal instruments need to be analysed to test whether provisions are adequate to combat cybercrimes through social media.

This paper mainly tries to ascertain the effectiveness of the present legal framework on cybercrime through social media in Bangladesh and to proffer recommendations and solutions to identified problems and loopholes. In this regard, this paper includes some examples of cybercrimes for showing that how cybercrime is occurring in our society through social media. To combat cybercrime in social media especially in Facebook how much effective is the Digital Security Act and ICT Act is a great concern of this study.

The paper is based both on the primary and secondary sources. The main authoritative sources of this paper have been drawn from legislations, internet materials and journal articles. As such, section 2 of the paper discusses what the cybercrime through social media is and how this crime is expanding in Bangladesh. In section 3 how cybercrime is occurring in our society by using social media has been drawn with some recent incidents of cybercrimes. Section 4 includes the existing legislations and bodies dealing with cybercrime in Bangladesh and successively section 5 analyses existing legal frameworks on cybercrime especially the ICT Act 2006 and the Digital Security Act 2018. Finally section 6 proposes a new law for combating cybercrimes aiming to establish safe social media and restraining of its misuse by users. The name of such a statute can be 'Safety of Social Media and Misuse Restraint Act' and we as such proposed some recommendations about this suggested statute.

Although the paper discusses about cybercrime occurred through social media but it mainly focuses on Facebook. As among six major social media used herein Bangladesh, Facebook covers more than 97%, so this paper vitally focused on this social media. Australia recently passed Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 to prevent 'abhorrent violent conduct' shared in social media and this Act provides that any such violent conduct must be removed from social media platforms. Many other countries are also thinking about enacting law to prevent cybercrimes occurred through social media.

2.0 The Notion of 'Cybercrime through Social Media' and its Expansion in Bangladesh

Cybercrime is such a nature of crime that cannot be described as a single definition rather it is best considered as a collection of acts or conducts. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. This crime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc.

Before introducing of social media, no one has thought much about 'cybercrime through social media' but once social media got into light cybercrime has also been happening by using it. Hence, in this paper 'cybercrime through social media' is termed as those crimes which have also been defined as crimes under general law of Bangladesh. When an offline incident of harassment is happening in society it is a crime under general law but when it is happening through social media, it can be termed a 'cybercrime occurred through social media'. Henceforth, the notion of 'cybercrime through social media' is getting strong look with time but we can define now the term likely that 'crimes which are occurring by users of social media where these social media are being used as a tool to commit those crimes'.

'Cybercrime through social media' is expanding rapidly in Bangladesh as almost fifty percent people of Bangladesh are now using social media as a tool of communication. In this paper, we mainly focused on Facebook but statistics show that Facebook, YouTube, Pinterest, Twitter, Instragram and reddit are now being widely used here in Bangladesh. These social media has been on rise in past several years, which changes the communicational landscape of general people.

Facebook	97.23%
YouTube	1.41%
Pinterest	0.63%
Twitter	0.35%
Instagram	0.29%
reddit	0.03%

Social Media Stats in Bangladesh - January 2020[3]

[3] Statecounter (Global Stats) <www.gs.statcounter.com/social-media-stats/all/bangladesh> accessed 20 February 2020.

How much speedily cybercrime is expanding in Bangladesh, is a great concern to everyone. According to one survey of 2017, Dhaka held the second highest number of active Facebook users, worldwide.[4] Accordingly it is true that social media users especially Facebook users are increasing so speedily that now a Facebook account has become an alternative identity of someone's National Identity (NID) card! These users are occurring cybercrime roughly and the key motives of such cybercrimes are defaming the victim, religious comments, revenge, obsession for love and emotion, trafficking, spreading fake and fabricating news, hate crimes, telemarketing and internet fraud, identity theft, harassment and stalking, credit card fraud, etc.

Cybercrimes are taking place every day in the country. A total of 2,044 cases were filed with different police stations and the lone cyber tribunal in the last six years, according to the Cyber Tribunal (Bangladesh) in Dhaka. Data shows the tribunal received 925 cases in 2018 while 130 cases in the last two months (January-February) of 2018. The number of cybercrime related cases has increased many folds in the last six years as the number of cases increased to 925 in 2018 from only three in 2013. Although cybercrime cases were only three in 2013, it increased to 33 in 2014, 152 in 2015, 233 in 2016, and 568 in 2017.[5]

3.0 How Cybercrime is Occurring through Social Media?

> For 16-year-old Rabeya living in a small town in Sylhet, the introduction of the Internet was a blessing in many ways. With strict parents who did not allow her to go out of the house alone, she was glad to have access to another world where there was no one overseeing her interactions or telling her what to do. Before long, she developed a relationship with a man who claimed to be working in a bank in Dhaka, with whom she shared intimate details of her life. After a few months of chatting, he demanded that she send him explicit pictures of herself. When she refused, his whole demeanour towards her changed; he began to send her highly inappropriate images and videos and make derogatory comments about her appearance and character. As Rabeya tried to block and delete

[4] Hasan Tasnim Shaon, 'Misuse of social media on the rise' the Daily Star (Dhaka, 1 June 2019) <www.thedailystar.net/letters/news/misuse-social-media-the-rise-1751680> accessed 25 December 2019.

[5] Md Sanaul Islam Tipu, 'Over 900 cases related to cybercrimes filed in 2018' DhakaTribune (Dhaka, 21 April 2019) <www.dhakatribune.com/cybersecurity/2019/04/21/over-900-cases-related-to-cybercrimes-filed-in-2018> accessed 26 December 2019.

> him from his friend list, he threatened to call her parents and tell them what a 'whore' she was.[6]

This is an example of how cybercrime is occurring through social media. If we look at past some years we see that a lot of cybercrime has been reported and some of them burst out in media. Hereafter in this paper, we have cited some of these occurred incidents of cybercrimes which are often happening in our society by using social media for understanding that how cybercrime is happening in our society through social media and these cybercrimes may be as follows:

3.1 Fraud & Cheating

Online fraud and cheating via social media is one of the most lucrative businesses that are growing today. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc. Most of the business owner is willing to do marketing via giving advertisement on social media and few fraud people is taking this opportunities to cheat users. We may illustrate an example here:

> Suppose an advertisement on Facebook is saying 'if you buy one product from our site then you'll get five more products absolutely free'. Now this is definitely an eye catchy offer and naive user will go on the site and buy product while giving their credit card information to get those free product.

Thus their credit card information is stolen.

Here we will cite a true incident of fraud through social media reported in Dhaka Tribune in 12 May 2019.[7] The accused fraud, Abdus Salam Polash, was the owner of Rex IT Institute which did provide IT based training in Dhaka. He had been arrested on charges of misappropriating 200 crore of money from investors and clients by digital fraud, that includes digital marketing and transactions. The company first lured investors into the digital world using free marketing techniques. Then they provided lucrative offers paid marketing through social media platforms. They would offer 50% to 100% return on investment to investors in the company. Over five thousand trainees at the company were convinced to invest in this manner and they became victim of such fraud.

---

6 Sushmita S. Preetha, 'Digital Sexual Harassment in Digital Bangladesh' the Daily Star (Dhaka, 16 May 2015) <www.thedailystar.net/in-focus/digital-sexual-harassment-digital-bangladesh-82480> accessed 13 October 2019.

7 Abdullah Alif, 'Man held for digital fraud and embezzlement of Tk200cr' DhakaTribune (Dhaka, 12 May 2019) <www.dhakatribune.com/bangladesh/dhaka/2019/05/12/man-held-for-digital-fraud-and-embezzlement-of-tk200cr> accessed 12 October 2019.

3.2 Trafficking

Now-a-days, social media is also used as a channel for human trafficking. This is a regular scenario for the recent times around the world and, accordingly in Bangladesh, this practice has already started. Love affairs, promise of marriage, fraudulence etc. have become the scenario of this human trafficking. For this national and international human trade, the traffickers adopt some strategies through social media. Sometimes it is seen that people get into several love affair relationships through social media. They even do not see each other, do not know each other, but get into relationship through trust. But some fraud traffickers pretend to be in love with young girls and asking them to elope. The girls believe them and leave their parents/home with their boyfriends full of illusions about a happy married life. Thus they get caught.

A report was published on 31st July of 2018 in the Daily NEWAGE Bangladesh heading that 'traffickers now using social media to allure girls'. In the report the correspondent citing Professor Ishrat Shamim of Sociology Department of Dhaka University reported that traffickers 'now use social media' befriending easy targets such as children and women through Facebook, Twitter, Instragram, Snapchat. The victims 'are trafficked' within countries, between neighbouring countries and even across different continents as cross-border trafficking 'flows often resemble' regular migration flows, she said.[8] According to Bangladesh Police Headquarters, a total of 4,152 cases were filed since the enactment of the Prevention and Suppression of Human Trafficking Act 2012.[9]

3.3 Fabricating News

Fake and fabricating news has been a hot topic in the last few years. A report of the Daily Sun shows that cyber security experts say dishonest people spread fake news through social media in crisis periods of the nation to create anarchy in the country.[10] Some news portals carry such fake news found in social media posts and accordingly many people share that news on the social media without verifying the authenticity. During

---

8 Staff Correspondent, 'Traffickers now using social media to allure girls' NEWAGE Bangladesh (Dhaka, 31 July 2018) <www.newagebd.net/article/47315/traffickers-now-using-social-media-to-allure-girls> accessed 25 December 2019.

9 ibid

10 ANM Mohibub Uz Zaman, 'Fake news on social media a great threat to country's stability' Daily Sun (Dhaka, 25 April 2018) <www.daily-sun.com/arcprint/details/304499/Fake-news-on-social-media-a-great-threatto-country%E2%80%99s-stability/2018-04-25> accessed 25 December 2019.

the some recent past years, we have noticed incidents of rumours in social media.

> Here we can take the example of 'salt' case. We have seen that after spreading the fabricating news of salt crisis, how the price of it soared across the country following the start of panic buying of the essential item after a rumour spread that its price, too, might skyrocket like that of onion.

3.4 Offensive Statements

Recently, offensive statements by users in social media have become very common and usual factor. These offensive statements and comments in social media include defamation, hate speech, statement against the State or the Government 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'. A report in the Dhaka Tribune[11] shows that the Counter-Terrorism and Transnational Crime (CTTC) cyber unit has identified around 2,500 Facebook pages which are fanning communal hatred in Bangladesh by spreading hate speeches.

Here we can cite an example of in reality:

> Monirul Islam, a rubber plantation worker in Srimongol, was arrested on April 13, 2017, accused of defaming the country's prime minister and harming the image of Bangladesh. His crime: he had 'liked' and then 'shared' a Facebook post, something social media users around the world do every day. The post, allegedly from a colleague, criticized the ongoing visit by Prime Minister Sheikh Hasina Wazed to India, saying that she was meeting her Indian counterpart, 'for the sake of power and to win the coming election'. The post included some cartoons of the prime minister. He was accused of offences under section 57 of the ICT Act claiming that he, and the publisher of the post, were 'opposition supporters' and that the post was an 'injustice', 'condemnable', and a 'betrayal to the country'. Denied bail by both the magistrate and district courts, Islam, who denies the offence, was detained for three months before the High Court released him in July 2017. Meanwhile, the author of the original post reportedly went into hiding fearing his own arrest.[12]

---

11 Kamrul Hasan, '2,500 Facebook pages spread communal hatred in Bangladesh' DhakaTribune (Dhaka, 16 November 2019) <www.dhakatribune.com/bangladesh/2017/11/16/hundreds-facebook-pages-spreading-communal-hatred-bangladesh> accessed 28 December 2019.

12 'No Place for Criticism: Bangladesh Crackdown on Social Media Commentary' <https://hrw.org/report/2018/05/09/no-place-criticism/bangladesh-crackdown-social-media-commentary> accessed 31 December 2019.

3.5 Identity Theft

Identity theft occurs when a person uses the social media to steal someone's identity and it is very precarious cybercrime that has grown at surprising rates over the past few years in Bangladesh. Researchers describe identity theft as an attempt of getting personal information of an individual for a criminal activity.

We can take recent example of music director Sazid Sarker:

> Sazid Sarker is a famous music director and composer of Bangladesh but listeners do not know much about him. A fraudster namely Sobuj Shikder used to upload popular tracks composed by Sazid Sarker on his Facebook account, opened in the name of Sazid. He used to contact upcoming singers and models on Facebook messenger and demand money and lured them to do immoral acts in exchange of giving them chance to sing for him. This fraudster (Shobuj Shikder in the name of Sazid Sarker) was later arrested in Dhaka by Cyber Security and Crime Division of Dhaka Metropolitan Police (DMP).[13]

3.6 Cyberbullying

Cyberbullying is not just an act to be scorned upon but is an abundant offence. Cyberbullying can cause profound harm as it can quickly reach a wide audience, and can remain accessible online indefinitely, virtually 'following' its victims online for life. A few examples of cyberbullying are, causing someone harm by posting unwanted or private information, threatening a person by sending mean messages via messenger, emails, social networking sites, text or audio messages, sharing private or embarrassing pictures, etc. A recent study titled, Online Safety of Children in Bangladesh, commissioned by UNICEF Bangladesh, surveyed 1281 school-going children (aged 10 to 17) from school, college, Madrasah and UNICEF calls for concerted action to prevent bullying and harassment for the 32 percent of children in Bangladesh.

3.7 Stalking

Incidents of cyber stalking are increasing at a rapid rate in Bangladesh. In the overwhelming majority of the cases women and young girls are the victims. Though history tells us that stalking is not just a modern phenomenon, new technology has added some special dimensions. This old crime got new look just because of social media. Sometimes criminals

---

[13] Bangladesh Sangbad Sangstha, 'Fake music composer arrested' NEWAGE Bangladesh (Dhaka, 16 February 2020) <www.newagebd.net/article/99731/fake-music-composer-arrested> accessed 22 February 2020.

take pictures or collect pictures from Facebook of female students and then write blogs to publish or distribute the obscene content in Facebook to embarrass them. According to the media, many victims keep quiet to avoid embarrassment and a few become mentally imbalanced. Cyber-stalkers are well aware about such stalking and do it deliberately. This stalking by using the social media may cause feelings of irritation, abuse and emotionally anxiety to the victim. In order to harass a woman her telephone number is given to others as if she wants to be friends with males.

3.8 Harassment

Online harassment is prevalent across different kinds of communication channels and social media. Such harassing behaviours include (but not limited to) sending sexually explicit messages to someone without their prior consent, using private pictures to blackmail, demeaning someone because of their gender, attacking someone using explicit words before the public, etc.

Responses Regarding Harassment	Yes	No
Facing harassment	36.8%	63.2%
Harassment from new people	21.1%	84.2%
Unusual situations treat as harassment	26.3%	78.9%
Harassment from different perspectives	42.1%	57.9%

Responses due to Harassment in Facebook[14]

Dhaka Tribune published a report in September 21 of 2017 heading ‘women biggest victims of rising cyber crimes’ that:

> In mid-August of 2017, Rapid Action Battalion (RAB) arrested two mobile phone repairmen, Sabuj and Madhu. They were found guilty of using their jobs to acquire personal information and content from various women. The two men would take these files from the mobile phones of women who brought them in for repair. They also accessed their IMO messenger apps and ran them in parallel on their own devices, reading

[14] Sabbir Ahmed et al, ‘Cyber-crimes Against Womenfolk on Social Networks: Bangladesh Context’ (2017) 174(4) International Journal of Computer Applications <https://file:///C:/Users/BiLD01/ Downloads/Cyber-crimes_Against_Womenfolk_on_Social.pdf> accessed 27 December 2019.

personal messages. The duo used all this information to blackmail a number of women.[15]

3.9 Obscene and Offensive Content

A news report published in the Financial Express in January 26, 2019[16] shows that Counter Terrorism and Transnational Crime (CTTC) arrested two youths on charges of demanding money from the people after threatening them to make viral their fake nude pictures and videos on social networking sites. These two youths were arrested under the Digital Security Act. The complainant alleged that the arrestees have opened two fake Facebook IDs after his name and later sent his fake nude pictures and videos to his messenger thorough his Facebook ID and demanded Tk 12,000 for not uploading those to internet.

In September 2012, Buddhist temples in Ramu were burnt to the ground. It was originated from a local Buddhist, Uttam Kumar Barua being tagged in a Facebook image of Quran. An unknown/fake Facebook user, using a pseudonym, posted burning-Quran image on Uttam Kumar Barua's Facebook wall. Reacted by the post, a group of arsonists put fire at the Buddhist temple. Fanatics attacked the Buddhist community in Ramu, claiming that a Buddhist youth insulted Islam on social media.[17]

4.0 Existing Legal Frameworks of Bangladesh

The aim of this section is to discuss the legal framework on cybercrime in Bangladesh. Hence we have considered all the legislations including statutes, rules, regulations, guidelines, strategy and concerned regulatory bodies dealing cybercrimes in Bangladesh. We have encompassed the Bangladesh Telecommunication Regulation Act 2001, the Information and Communication Technology Act 2006, the Pornography Control Act 2012, the Prevention and Suppression of Human Trafficking Act 2012, the Digital Security Act 2018, the Information Security Guidelines 2014 and the National Cyber Security Strategy of Bangladesh 2014. Although we

---

15 Arifur Rahman Rabbi, 'Women biggest victims of rising cyber crimes' DhakaTribune (Dhaka, 21 September 2017) <www.dhakatribune.com/bangladesh/crime/2017/09/21/women-biggest-victims-rising-cyber-crimes> accessed 27 December 2019.

16 'Police arrest youths for blackmailing on Facebook' the Financial Express (Dhaka, 26 January 2019) <www.thefinancialexpress.com.bd/national/crime/police-arrest-youths-for-blackmailing-on-facebook-1548498221> accessed 17 December 2019.

17 Star Report, '12 BUDDHIST TEMPLES TORCHED, 50 HOUSES SMASHED: Extremists 'linked'' the Daily Star (Dhaka, 01 October 2012) <www.thedailystar.net/news-detail-251955> accessed 23 December 2019.

discussed the abovementioned legislations with some others but we did not apprise all of those rather we made comprehensive appraisal of the ICT Act 2006 and the Digital Security Act 2018 and slightly the Telecommunication Regulation Act 2001. Next to the legislations, we included here in this paper some concerned regulatory bodies which deal with the prevention of cybercrimes. Bangladesh Telecommunication Regulatory Commission is the main concerned body which play a vital role in this regard. Furthermore, there have numerous bodies including Information and Communication Technology Department, Computer Security Incidence Response Team (CSIR Team), Digital Security Agency (DSA), National Computer Emergency Response Team (CERT), DMP Cyber Crime Unit, Cyber Security and Crime Division, etc.

4.1 Current Legislations Regulating Cybercrime in Bangladesh

In 2001, Bangladesh Telecommunication Regulation Act was enacted to stop any sort of unintended cyber incidents with the use of telecommunication tools. At that time no social media was invented and came to light and hence the Act does not think about cybercrime through social media but it had provision that cybercrime through internet via telecommunication medium would be punished under the law. The Act has created a powerful regulatory authority in the telecommunication sector and section 53 of the Act gives the sector ample power to intercept the communication system to stop any sort of unwanted cyber incidents with the use of telecommunication tools in the country.

Later, in 2006 the government enacted the Information and Communication Technology Act. The Act provides law-enforcing agencies the authority to investigate an offence and bring the offender to book under a special court of law known as the Cyber Tribunal. For the sake of quick action, the Act has given concerned authority ample power to arrest the offenders and seize, confiscate or otherwise dispose the properties involved in these crimes. The Act has created an office of the Controller of Certifying Authorities (CCA) with a view to promoting e-commerce through extensive use of electronic signature properly certified by licenced authorities. In 2013, the Government of Bangladesh introduced an amendment to the said ICT Act of 2006 that changed the complexion of criminal prosecution for online offences under the Act. Offences under the Act were made cognisable, which meant police could pursue investigation and arrest suspects without a court-issued warrant.

Additionally, the amendment set up a special tribunal known as the Cyber Tribunal to try cases under the ICT Act. The Tribunal was set up with stringent guidelines on the time it had to clear cases in an attempt to

increase conviction rates. During the initial years of establishment of the Tribunal, a surprisingly low number of cases were actually filed in court. In the first three years of its establishment, there were under 200 cases filed under the Tribunal. The rate at which cases have been cleared have also been problematic, with reports suggesting the conviction rate of the Tribunal stood at 3% till 2019. Of the cases presented to the Tribunal, the police filed a final investigation report for only 26% of cases, of which nearly 65% could not be tried as the probes were found to be carried out in disregard of proper procedure. A special public prosecutor for the Cyber Tribunal also claimed that the reports filed by the police had a lack of digital forensic evidence due to which the prosecution could not build a credible case and the accused was acquitted after the trial. The issues with processing such cases have been further compounded by the fact that most records of the Cyber Tribunal are not available publicly.

Furthermore, the ICT Division has formed the Information Security Guidelines 2014 and the National Cyber Security Strategy of Bangladesh 2014. Under these guidelines, national data centre located in BCC Bhaban has been equipped with necessary tools for proper storage and monitoring of data.

Later in September of 2018, Bangladesh enacted the Digital Security Act. Passed with the objective of curbing cybercrime and ensuring digital security, the Act creates a wide range of cybercrime offences. These provide punishment for propaganda or campaign against the Liberation War, the Father of the Nation, posting offensive content, cyber terrorism and defamation, amongst others. Significantly, it has extra-territorial application. It also establishes a 'Digital Security Agency', empowered to regulate content and request the Bangladesh Telecommunication Regulatory Commission remove or block the same.

Cyber pornography can be prosecuted by section 8 of the Pornography Control Act 2012. It will be extremely difficult to prosecute an act of morphing if the morphed image or video does not fall within the meaning of pornography. Acts of cyber stalking will probably continue to be immune from legal process as these laws do not specifically define them and our trial judges will rationally be reluctant to convict a person for acts not defined as crimes. The government has adopted a cyber-security declaration 2017 asking organizations to develop actionable cyber security road maps to be approved and monitored by the top management.

Under the existing laws of Bangladesh, any kind of online expression that is false, obscene, defamatory, hurtful to religious sentiment, likely to hurt the image of the nation, or constitutes pornography is a criminal offense.

Those responsible can be prosecuted for such online offences either in the cyber tribunals.

In a nutshell-

Telecommunication Regulation Act 2001 provides for the establishment of an independent Commission for the purpose of development and efficient regulation of telecommunication system and telecommunication services in Bangladesh and matters ancillary thereto.

ICT Act sets penalties for cybercrimes in order to facilitate e-commerce and encourage the growth of information technology.

The Digital Security Act 2018 (a) created Digital Security Agency to oversee and enforce provisions in the Act; (b) outlined role of National CERT in responding to and mitigating cyber incidents; (c) created Digital Forensic Lab; (d) created a National Digital Security Council; and (e) criminalized a wide array of cyber activities, including hacking, identity fraud, and damaging infrastructure, as well as influencing activities such as disseminating propaganda or offensive material.

4.2 Regulatory Bodies dealing Cybercrime in Bangladesh

The BTRC, established under the Bangladesh Telecommunication Regulation Act of 2001, is the official regulatory body overseeing telecommunication and related ICT issues. This commission blocks inappropriate websites, blogs, and Facebook accounts. Authorities amended the Act in 2010, passing telecommunications regulation to the Ministry of Post and Telecommunications and making the BTRC an auxiliary organization.

The Digital Security Act 2018 establishes some authority and regulatory bodies in this regard. Section 5 of the Act establishes the Digital Security Agency (Agency) as the key institutional structure for implementing the law and the Digital Security Act is, in turn, overseen by the National Digital Security Council, established by section 12. The Digital Security Council is formed consisting of 13 (thirteen) members including a chairman. Not only has that section 9 made provision that there will have a National Computer Emergency Response Team (CERT).

Bangladesh police have opened a cyber-wing to deal with the increasing number of cyber threats and it is responsible for monitoring cybercrimes and tracking the criminals. Bangladesh Police have also a special branch named ‘Anti-cyber Crime Department’ headed by the Deputy Commissioner of Police to protect e-mail fraud, treat by e-mail, defamation or publishing of unauthorized pictures.

Some authority and regulatory bodies listed below:

✓	Bangladesh Telecommunication Regulation Communication (BTRC)
✓	Information and Communication Technology Department
✓	Computer Security Incidence Response Team (CSIR Team)
✓	Digital Security Agency (DSA)
✓	National Computer Emergency Response Team (CERT)
✓	DMP Cyber Crime Unit
✓	Counter Terrorism and Transnational Crime (CTTC) (run by DMP)
✓	Cyber Security and Crime Division (run by Bangladesh Police)

5.0 Analysis of Existing Laws

In this section, we have basically analysed the ICT Act 2006 and the Digital Security Act 2018. We have to acknowledge that Bangladesh has gone more ahead in restricting cybercrimes by enacting anti-cybercrimes legislations in due time. But the laws are hazardous and more complicated and at the same time the laws do not especially mention anything about cybercrimes committed by use of social media. Some foreign countries already took measure and many are thinking about promulgating such kind of law.

The ICT Act has provided us various advantages like conduct important issues with security. The Act promoted e-commerce and recognized email, digital signature, online contract as valid. It ensures secure corporate business by issuing digital signatures and certificate by certifying authority. The 2006 Act provides power to penalize the cyber-criminal and tackles the cybercrime. The Act ensures legal status of the online transaction but it has at the same time been supporting legislation that seeks to undue limit freedom to use digital communications technologies.

However, the Digital Security Act contains far more and far more problematical provisions which introduce unduly limiting restrictions on digital content, create a number of vastly overbroad other criminal offences relating to digital technologies and give government controlled bodies extensive power over digital communications.

Although proper execution of statutes ensures the rule of law but there have lacking of proper execution of these statutes. Circumstances say that inadequate execution of the ICT Act 2006 is one of the root causes for the increasing cybercrimes in Bangladesh.

5.1 Restraint of Publishing Fake, Obscene or Defaming Information

Unfortunately, the Digital Security Act 2018 expands existing restrictive provisions and it includes several provisions that are too vague and overbroad. It contains several speech offences, including criminal defamation, defamation of religions, or the sending of 'offensive' information that would criminalise a wide range of legitimate expression.

In the original version of the ICT Act 2006, publishing fake, obscene or defaming information was a bailable offence (i.e. bail would normally be granted pending trial) and non-cognizable (the police could not act on a complaint without getting approval from the Licensing Authority as defined in the Act). The maximum penalty was ten years' imprisonment and/or a fine of BDT 10,000,000. Amendments introduced in 2013 made this offence non-bailable so that, once charged and taken into custody, an accused will be held in detention until and unless a court, in its discretion, agrees to grant bail. Furthermore, the offence was rendered cognizable, so that the police can accept complaints (FIRs or First Information Reports) and arrest the accused without a judicial warrant. Finally, the system of penalties was substantially revised, with a minimum sentence of seven years' imprisonment being established, alongside a maximum of 14 years, while the fines were retained. These key features – and especially non-bailable status and minimum terms of imprisonment – are normally reserved for the very most serious crimes.

Section 57 (now repealed) of the ICT Act 2006 is as follows:

> 57. Punishment for publishing fake, obscene or defaming information in electronic form.-
> (1) If any person deliberately publishes or transmits or causes to be published or transmitted 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.

According to the ICT Act 2006, it is a crime to release one's personal photo on the internet, no matter how, when and why it was taken. But photos of victim, mostly the ones taken in close proximity during any emotional time, are uploaded on the internet in an effort to blackmail, creating an embarrassing situation not only for the victim, but also for the

family. In most cases, the victims do not want to take recourse to law for various reasons, including social humiliation.

5.2 Preventing Online Harassment

Bangladesh enacted ICT Act in 2006 to combat cybercrime and online harassments. However, the provisions of this Act are quite insufficient to undertake legal measures appropriately as it does not address gender-based violence online in a clear and effective manner. Similarly, the Bangladesh Telecommunication Regulation Act 2001 does not address the gender-based violence that occurs via the use of telecom networks or the internet. The Pornography Control Act is not properly used to combat cyber violence because of the institutional corruption and powerful allies with the ruling politics. The influential remains safe always if the victims are poor.

5.3 Hate Speech and Defamation

Sections 28, 29 along with 31 of the Digital Security Act 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, defense, 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 international obligation of the government of Bangladesh and to bring to book the offender without unnecessary delay.

Unfortunately, not only does the 2018 Act expand existing restrictive provisions, it includes several provisions that are in breach of international human rights law. In particular, several definitions contained in the 2018 Act are too vague and overbroad. Summarized in brief:

- The Act vests sweeping blocking powers in a government agency.
- It contains several speech offences, including criminal defamation, defamation of religions, or the sending of 'offensive' information that would criminalise a wide range of legitimate expression.
- It grants carte blanche to the government to make rules in areas such as the collection, preservation or decryption of evidence or data, rules that ought to be decided by the Bangladesh Parliament with a view to protect the rights to freedom of expression, privacy and due process.

5.4 Block or Remove Content

Section 8 of the Digital Security Act grants enormously wide powers to block or remove content, which is a very intrusive power, but says almost nothing about how this will work. Instead, section 8(4) provides: to fulfil the objective of this section, other relevant matters will be determined by the Rules. Once again, at least a framework of procedures governing the exercise of this power should be set out in the primary legislation.

Operationally, this becomes very important, for example in section 8(1), which gives the Director General of the Digital Security Agency, the key implementing body for the legislation, created by section 5 of the Digital Security Act, the power to request the Bangladesh Telecommunication Regulatory Commission (BTRC) to remove or block any information or data that 'poses a risk to digital security'. Similarly, section 9 establishes a National Computer Emergency Response Team, a group of experts on digital security and law working under the Agency. According to section 9(5)(b), this Team can take 'necessary steps to protect the information infrastructure' if digital security is at risk. And again, the National Digital Security Council, an oversight body created by section 12 of the Act, can issue 'necessary directives if digital security is at risk'.[18] In all of these cases, a far narrower definition, with higher minimum thresholds, is needed.

5.5 Failure of Regulatory Bodies

The National Computer Emergency Response Team is allocated a number of very general powers, such as to take 'necessary measures to prevent possible or upcoming cyber or digital attack'. Once again, a catch-all is provided, with section 9(5)(e) of the Digital Security Act providing that the Team shall undertake 'any other activity directed by the Rule'. Similarly, important matters relating to the Digital Forensic Lab[19] and the National Digital Security Council[20] are left to be determined by the rules. Another body created by the Act which is described in more detail in the section of this Analysis on Institutional Structures and Independence. Similarly, section 6 of the Bangladesh Telecommunication Regulation Act 2001 establishes the Bangladesh Telecommunication Regulatory Commission, and its objectives, functions and powers are described in great detail respectively in sections 29, 30 and 31. Thus, the Act deviates from established practice in Bangladesh by failing to define properly the

18 The Digital Security Act, s 13(2).

19 ibid, ss 10(4) and 11(1).

20 ibid, s 13(2)(e).

functions and powers of the bodies it creates and, instead, leaving this to be determined by the government.

5.6 Offences committed via Websites or Other Digital Platforms

Section 25 of the Digital Security Act creates a number of offences committed via websites or other digital platforms, including: purposefully publishing or broadcasting 'offensive or intimidating' information;[21] publishing information that 'can make a man corrupt or degraded';[22] publishing or broadcasting information one knows to be false to 'annoy, humiliate, insult someone';[23] or knowing it to be false or propaganda, publishing information, 'either in full or partially distorted to tarnish the image or the good name of the State'.[24]

5.7 Absence of Definition and Inclusion of Social Media in the Acts

None of the Act ever defines what cybercrime is. Even the mother law i.e. the ICT Act 2006 is not comprehensive enough and doesn't even define the term 'cybercrime'. Social Media as a tool of cybercrime should be especially mentioned and included but none of Act included this. The main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the ICT Act 2006 was passed, which also is one of the reasons for its inadequacy to deal with cases of cybercrime.

5.8 Lacking of the Remedies

Prevention is better than cure and for prevention of numerous cybercrimes it is better to initiate advanced technological actions. These are technological precautionary affairs for prior prevention. Through the ICT Act 2006 it is being tried to locate all the probable grounds of cybercrime frequently occurring at present and which might occur in future as well. Moreover as per the provisions of the ICT Act a good number of other procedural and structural hurdles also exist which are as follows: *firstly*, in tribunal procedure, judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes. *Secondly*, a police officer not below the rank of a Sub-Inspector can be the IO (Investigation Officer) regarding the cybercrimes. Like the judges, police officers also have no

---

21 ibid, s 25(1)(a).

22 ibid, s 25(1)(b).

23 ibid, s 25(1)(c).

24 ibid, s 25(1)(d).

opportunity to gather the required technological knowledge due to the lack of proper initiatives. There is no provision for them to be assisted by any ICT expert like the judges of Cyber Appellate Tribunal. *Thirdly*, the government bears the responsibility not only of forming the cyber tribunals but also of preparing terms and conditions of the service of the judges of those proposed tribunals. Regrettably neither a single rule has been framed nor has a project or a proposal been taken or passed so far by the state.

5.9 Section 38 and Service Providers

Section 38 of the Digital Security Act is essentially a positive provision, inasmuch as it provides protection to a service providers as long as it can prove that it was 'not aware of the offence or tried its best to prevent the commission of offence'. Unfortunately, the conditions upon which responsibility arises are too broad. For example, if someone complains to a service provider that content in relation to which they provide services is defamatory, are they deemed to be 'aware of the offence' if it should ultimately prove that the material is in fact defamatory? The problem with this is that service providers are not legal experts or in a position, unlike traditional publishers, to stand up for the (often vast numbers of) information transactions that run through their services. If they bear a potential risk of liability, then they will simply take action to block or remove the content so as to meet the condition of doing their 'best to prevent the commission of offence'. In effect, this turns everyone into a censor because all one has to do is make an allegation of illegality in relation to content to have it taken down.

Taking action in the context of a mere allegation of wrongdoing can lead to abusive results. For example, in the United States, in one case someone claiming to have psychic powers objected to YouTube when someone else uploaded a clip from a television programme showing how the actions performed by the psychic could easily be done without any special powers. YouTube not only took the post down but also suspended the person's account for two weeks, until their counter-claim was processed.

5.10 Cyber Tribunal

According to section 68 of the ICT Act 2006, for the speedy and effective disposal of cases under this Act, Government shall establish one or more cyber tribunal. The tribunal shall try only the offences under this Act and the Government shall determine the local jurisdiction of the tribunal. In consultation with the Supreme Court, Government shall appoint on Sessions Judge or Additional Sessions Judge as a judge of Cyber Tribunal. Cyber tribunal shall take a case for trial – a) upon the report of a police

officer not below the rank of sub-inspector or b) upon a complaint made by a controller appointed under this Act or by any other person authorized by the controller. Tribunal shall conclude the trial within six months from the date of framing charge. This period may be extended for three months. Tribunal shall pronounce its judgment within ten days after the conclusion of trial which may be deferred for ten days. The Digital Security Act followed the ICT Act in establishing special court as crimes under both the Acts would be in trail of the same Cyber Tribunal.

5.11 Weakness of Law

Under the ICT Act 2006 the victim has to file an allegation to the law enforcing agencies to get remedy. This is the main weakness of the said Act. In the time of enactment of the said Act it was said in section 68 that a special tribunal named Cyber Tribunal will be established in every district of Bangladesh. But till now only a tribunal has been established in capital city Dhaka. Because of the dependency of technology specialist and well trained lawyer and judges the disposal of cyber cases are rare. To remove such kind of pendency of cases judges, lawyer and specialist should be well trained.

The Digital Security Act does not indicate who most of the members of the Council will be or even how they are appointed but it is clear that it is not independent of government because the Chair is the Prime Minister ((section 12(2)). The government also constitutes the Agency, appoints the Director General and approves its organogram (sections 5(1), 6(2) and 7(1)). Two key institutions operate under the Agency, namely the National Computer Emergency Response Team, established by section 9, and the system of digital forensic labs, set out in section 10. It is difficult to say with precision exactly what these various bodies do because, as noted above, while some general functions and powers are set out in the Act, important parts of their powers and functions are to be included in the Rules. However, it is clear that these bodies will exercise important regulatory powers over digital communications tools.

Though these steps have brought some progress in combating cyber offence, still there is much room for improvement. For example, in Bangladesh computer related incidents are generally referred to BTRC or CCA, which might not be the right authority to handle such occurrences. If the CERT is in place, it will be able to handle all computer related offences promptly in a coordinated manner and better inform about it to the individuals or organisations that fall victim to cybercrimes.

6.0 Concluding Remarks & Recommendation

People use social media to express their thoughts regarding socio-economic issues, share events of their personal life and interact with each other. But on the other hand, social media is used by a criminal to commit crime, the same way the technology can be used to control, prevent, protect and investigate the crime. A report of Aljazeera shows that protest organizers heavily depend on social media sites, such as Facebook and Twitter.[25] The undoubted presence of a vast amount of harmful content in social media has naturally raised questions about the need to regulate 'new' law. This is very much an evolving issue even in the most developed countries, with much legislative and regulatory attention being devoted to it, as well as much criticism and even striking down of legislation by courts.

Hence, in this paper, we will suggest the government to regulate a new law for restraining the misuse of social media. This law can be, for example, 'the Safety of Social Media and Misuse Restraint Act'. This suggested Act can be purely a remedial legislation for users and completely a preventive measure on the foregoing matters by regulating social media. Such statute would not be effective if it is not property executed and applied, because proper execution of statutes ensures the rule of law. Circumstances say that inadequate execution of the ICT Act 2006 is one of the root causes for the increasing cybercrimes in Bangladesh.

The Republic of Philippines already passed an Act regulating the use of social media, prescribing penalties and for other purposes. This statute's name is the Social Media Regulation Act 2017. Australia recently passed Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 to prevent 'abhorrent violent conduct' shared in social media and this Act provides that any such violent conduct must be removed from social media platforms. According to the legislation, forms of media depicting terrorism, murder, attempted murder, torture, rape and kidnapping, whether set within or outside Australia, is considered 'abhorrent violent conduct' and must be removed from social media platforms. Failure to do so 'expeditiously' could lead to companies having to pay a hefty fine of up to 10% of their annual profit, and employees imprisoned for up to three years. The law creates new offenses and liability, including imprisonment and huge fines for failing to take down violent content, such as the video of the Christchurch attack that was broadcast live on Facebook, quickly enough from online platforms.

---

25 A. J. A. AGENCIES, 'Timeline: Egypt's revolution', Al Jazeera, 2011.

Indian government is drafting guidelines that will bind companies such as Twitter, WhatsApp, YouTube and Facebook to respond to complaints over content in a few hours. Germany's NetzDG law came into effect at the beginning of 2018, applying to companies with more than two million registered users in the country. They were forced to set up procedures to review complaints about content they were hosting, remove anything that was clearly illegal within 24 hours and publish updates every six months about how they were doing. EU is considering a clampdown, specifically on terror videos. Social media platforms face fines if they do not delete extremist content within an hour. The EU also introduced the General Data Protection Regulation (GDPR) which set rules on how companies, including social media platforms, store and use people's data.

6.1 Recommendation

The current legislations of Bangladesh are wide but technically hazardous and complicated because of its redundant provision in various statues. So a special law regulating cybercrime in social media is necessary. Some foreign countries already took measure and many are thinking about promulgating such kind of law.

The explosion of online activity in recent has led to several pitfalls that need to be addressed, one of which is the abuse and misuse of social media which should be curtailed. The suggested 'Safety of Social Media and Misuse Restraint Act' can contribute to this curtailment.

The suggested Act seeks to afford a remedial measure on the foregoing matters and will regulate these social media by mandating the social media companies (Facebook, Twitter, YouTube, etc.) to reasonably verify the identity of user applicants before they are allowed to open an account. Penalties are also provided for failure to comply with this verification requirement. Likewise, those who steal someone else's identity shall also be penalized.

The suggested Act should be promulgated to protect information between different sources in order to enhance information and communications technology for national benefit. The users, who will communicate, exchange, deliver, blog, or share information through social media must observe a responsible and fair exercise of his right to free expression and opinion. He is, however, prohibited from opening an account for his online presence using someone else's identity and presenting himself to the online world as that person whom he is not.

The suggest Act also contain provision about responsibility of social media networks. The Act should have definition of social media and social media networks. It will contain penalties that any person who intentionally and maliciously commits any act in violation of provision would be punished.

REFERENCES

Legislations

- The Bangladesh Telecommunication Regulation Act 2001.
- The Digital Security Act 2018.
- The Information and Communication Technology Act 2006.
- The Information Security Guidelines 2014.
- The Pornography Control Act 2012.
- The Prevention and Suppression of Human Trafficking Act 2012.
- The National Cyber Security Strategy of Bangladesh 2014.
- The Social Media Regulation Act 2017 (Philippines).
- Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019 (Australia).

Others

- Ahmed S et al, 'Cyber-crimes Against Womenfolk on Social Networks: Bangladesh Context' (2017) 174(4) International Journal of Computer Applications <https://file:///C:/Users/ BiLD01/ Downloads/Cyber-crimes_ Against_Womenfolk_on_Social.pdf> accessed 27 December 2019.
- Alif A, 'Man held for digital fraud and embezzlement of Tk200cr' DhakaTribune (Dhaka, 12 May 2019) <www.dhakatribune.com/ bangladesh/dhaka/2019/05/12/man-held-for-digital-fraud-and-embezzlement-of-tk200cr> accessed 12 October 2019.
- Correspondent S, 'Traffickers now using social media to allure girls' NEWAGE Bangladesh (Dhaka, 31 July 2018) <www.newagebd.net/ article/47315/traffickers-now-using-social-media-to-allure-girls> accessed 25 December 2019.
- Hasan K, '2,500 Facebook pages spread communal hatred in Bangladesh' DhakaTribune (Dhaka, 16 November 2019) <www.dhakatribune.com/ bangladesh/2017/11/16/hundreds-facebook-pages-spreading-communal-hatred-bangladesh> accessed 28 December 2019.
- 'No Place for Criticism: Bangladesh Crackdown on Social Media Commentary' <https://hrw.org/report/2018/05/09/no-place-criticism/

bangladesh-crackdown-social-media-commentary> accessed 31 December 2019.

- 'Police arrest youths for blackmailing on Facebook' the Financial Express (Dhaka, 26 January 2019) <www.thefinancialexpress.com.bd/national/crime/police-arrest-youths-for-blackmailing-on-facebook-1548498221> accessed 17 December 2019).
- Preetha S S, 'Digital Sexual Harassment in Digital Bangladesh' the Daily Star (Dhaka, 16 May 2015) <www.thedailystar.net/in-focus/digital-sexual-harassment-digital-bangladesh-82480> accessed 13 October 2019.
- Rabbi A R, 'Women biggest victims of rising cyber crimes' DhakaTribune (Dhaka, 21 September 2017) <www.dhakatribune.com/bangladesh/crime/2017/09/21/women-biggest-victims-rising-cyber-crimes> accessed 27 December 2019.
- Report S, '12 BUDDHIST TEMPLES TORCHED, 50 HOUSES SMASHED: Extremists 'linked'' the Daily Star (Dhaka, 01 October 2012) <www.thedailystar.net/news-detail-251955> accessed 23 December 2019.
- Sangstha B S, 'Fake music composer arrested' NEWAGE Bangladesh (Dhaka, 16 February 2020) <www.newagebd.net/article/99731/fake-music-composer-arrested> accessed 22 February 2020.
- Shaon H T, 'Misuse of social media on the rise' the Daily Star (Dhaka, 1 June 2019) <www.thedailystar.net/letters/news/misuse-social-media-the-rise-1751680> accessed 25 December 2019.
- Statecounter (Global Stats) <www.gs.statcounter.com/social-media-stats/all/bangladesh> accessed 20 February 2020.
- Tipu M S I, 'Over 900 cases related to cybercrimes filed in 2018' DhakaTribune (Dhaka, 21 April 2019) <www.dhakatribune.com/cybersecurity/2019/04/21/over-900-cases-related-to-cybercrimes-filed-in-2018> accessed 26 December 2019.
- Zaman A M U, 'Fake news on social media a great threat to country's stability' Daily Sun (Dhaka, 25 April 2018) <www.daily-sun.com/arcprint/details/304499/Fake-news-on-social-media-a-great-threatto-country%E2%80%99s-stability/2018-04-25> accessed 25 December 2019.