Sonargaon University (SU)

Research Monograph

On

"Digital Security Act, 2018 of Bangladesh: A Study on the Press Freedom and Journalistic Investigation"

Research Paper submitted in partial fulfillment of the requirements
of the degree of LL.M (1 years) under Sonargaon University

Submitted To:

Sharmin Jahan Runa
Assistant Professor
&
Head (Acting)
Faculty of Arts and Humanities
Sonargaon University (SU)

Submitted by:

Md Rana
ID: LLM 2301028002
Batch : 28
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

Submission Date: 10th January, 2024

LETTER OF TRANSMITTAL

Date: 10th January, 2024

To

Sharmin Jahan Runa
Assistant Professor &
Head (Acting)
Faculty of Arts and Humanities
Sonargaon University (SU)

Subject: **Submission of Research Monograph on "Digital Security Act, 2018 of Bangladesh: A Study on the Press Freedom and Journalistic Investigation"**

Dear Madam,

It is a great pleasure to submit my thesis on. „**Digital Security Act, 2018 of Bangladesh: A Study on the Press Freedom and Journalistic Investigation**" I have given my best efforts to furnish the thesis with relevant information that I have collected from various ways. I have concentrated my best effort to achieve the objectives of the work and hope that my endeavor will serve the purpose. I will be highly grateful and obliged if you kindly accept my thesis and evaluate it with your sagacious judgment.

Sincerely Yours,

_____

Md Rana
ID: LLM 2301028002
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

ACKNOWLEDGEMENT

First I would like to thank the Almighty Allah, for accomplishing my thesis. Then I would like to show my guideline to **Sharmin Jahan Runa,** Assistant Professor & Head (Acting), Faculty of Arts and Humanities, Sonargaon University (SU) for giving me good guidance to accomplish my job. I would also like to extend my post gratitude to all who have directly or indirectly guided me in writing this thesis. Many people, especially my classmates and some seniors of my department; they gave me valuable suggestions on completing my work. The main goal of this law is to offer digital security and also detect, prevent and investigate the offences which correlate with the digital medium.

Md Rana
ID: LLM 2301028002
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

DECLARATION

I solemnly affirm and hereby declare that the thesis titled „**Digital Security Act, 2018 of Bangladesh: A Study on the Press Freedom and Journalistic Investigation**‟ is my original work and not submitted for the award of any other degree. Further undertake to indemnify the university against any loss or damage from breach of the forgoing obligation.

_____

Md Rana
ID: LLM 2301028002
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

CERTIFICATION

This is to certify that the research paper on: **"Digital Security Act, 2018 of Bangladesh: A Study on the Pres Freedom and Journalist Investigation"** is done by **Md Rana, ID: LLM 2301028002** in partial fulfillment of the requirement for the degree of LLM from Department of Law, Faculty of Arts and Humanities, Sonargaon University (SU). The dissertation has been carried out under my guidance and is a record of the bonafide work carried out successfully.

Sharmin Jahan Runa
Assistant Professor &
Head (Acting)
Faculty of Arts and Humanities
Sonargaon University (SU)

Abstract

The Act is enacted to ensure National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters. When the whole world is connected through the internet, it is so tough to protect privacy. Digital Security Act 2018 is such a law which protects the right to privacy of an individual .This Act refers to controls over personal information, controls over one's own body and control over personal dignity. This new law has however shown a more restrictive approach towards freedom of expression in its wordings and application than the former one. This excessive interference with free expression has encouraged demands frompeople of many walks for the abolishment of the DSA. The purpose of the law as mentioned in its preamble is to "ensure digital security and prevent crimes committed on digital platforms." Hence we should not have been worried about the law. But theproblem is that DSA goes much beyond its defined scope and ventures into the territoryof media and journalism. The law goes against the very nature and practice of independent journalism that stands to protect people's right to know and exposes abuse of power and corruption.

TABLE OF CONTENTS

Contents

Chapter 1 8
INTRODUCTION 8
1.1 Introduction 8
1.2 Research Objectives 9
1.3 Statement of Problem 9
1.4 Research Methodology 10
1.3 Limitations of the study 10
Chapter 2 11
The Concept of Freedom of Expression as Theoretical Framework 11
2.1 Concept of Freedom of Expression 11
2.2 Investigative Journalism 11
2.3 Concept of Digital Security 12
2.4 Digital Security Act 2018 12
2. Investigative Journalism 13
2.5 *Computers and the Internet* 15
Chapter 3 16
IMPACT OF DIGITAL SECURITY ACT IN BANGLADESH: FEARS AND PROTECTIONS 16
3.1 Investigative Reporting on Government and Its Activities 16
3.2 Investigative Journalism in Corporate Sectors 16
3.3 The Impacts and Fear of Digital Security Act on Investigative Journalism 17
3.4. The Fields of Protection by the Digital Security Act 20
Chapter 4 23
SUBSTANCE AND FEATURES OF DIGITAL SECURITY ACT, 2018 23
4.1 Enactment of the Act 23
4.2 Objects of the Act 23
4.3 Main features of this Act 25
4.4 Section 40 26
4.5 Section 41 26
4.6 Section 47 26
4.7 Section 52 27
4.8 Section 53 27
Chapter 5 29
PROBLEMS AND PROSPECTS OF THE ACT 29
5.1 Advantages of Digital Security Act 29
5.1.1 High Number of Offences 29
5.1.2 Disproportionate Sanctions 30
5.1.3 Exclusive Police Powers 30
5.2 Bangladesh parliament passes draconian Digital Security Act 30
5.3 New Digital Security Act imposes dangerous restrictions on freedom of expression 31
5.3.1 Lack of Procedural Safeguards for Human Rights Protection 32
Chapter 6 34
RECOMMENDATIONS AND CONCLUSION 34
6.1 Recommendations 34
6.2 The Cyber Security Bill 2023 35
6.3 Conclusion 37
Bibliography 39

Chapter 1
INTRODUCTION

1.1 Introduction

One fine evening, when one of the researchers went to take the interview of an editor of a media house and vice-president of a journalists" association, he agreed to talk with the condition of not disclosing his name. Showing the vulnerability he said, "You know the situation of the country. If I openly tell anything regarding the negative sides of the law, I would have to face embarrassing comments from higher authorities"'. Getting promise, he came up with lots of alarming situations of press freedom and freedom of expression such as the ownership pattern of the media, politicization of journalists and owners, threats and pressures from higher authorities and the legal situation as well. His expression of helplessness denotes the present situation of freedom o: expression in the country. An editor of a house who is also a leader of journalists' community; is feeling at risk andpress to -peak out on the regular problem the In the study, the situation of press freedom and journalistic investigation is studied where the aftermath scenario of passing theDigital Security Act (DSA) - 2018 was the main focus. Although the government and ministeis are citing freedom of press is safeguarded by the governments and the new law, DSA-2018, is a new accumulation to enrich it. But strong protests and criticism are coming from the journalists, freethinkers and right workers. This situation motivated to study whether the law is creating any barrier for investigative journalists or not.[1] The study revealed that journalists‟ basically investigative journalists are continuing their profession with the sense of fear and anxiety after passing the law which is ultimately resulting self-censorship and in the broader perspective it is contributing to curb the freedom of journalistic investigation as well as demining the standard of freedom of expression.[2]

[1] *Ibid.*

[2] Accessnow, (2018, August 10) Journalists, activists in Bangladesh arrested under ICT Act for posting on social media, Retrieved from https://www.accessnow.org/bangladesh-ict-act/

1.2 Research Objectives

1. To find out the Digital Security Act to limit journalistic investigation
2. To analyze the Bangladesh‟s Digital Security Act Is Creating a Culture of Fear
3. To minimize the offences, the government approved Digital Security Act (DSA) 2018
4. To analyze the journalists, right workers and activists became vocal against some sections of the law claiming those would hinder press freedom and freedom of journalistic investigation

1.3 Statement of Problem

Free press is one of the most important constituents of democracy as it assists to keep balance between government and mass. Bangladesh, a third world democratic country, ensured the freedom of expression in Article 39 of its constitution. But according to the World Press Freedom Index, 2019 by the Reporters Without Borders, the country is now 150th which arose doubt about the situation of freedom in the country. Besides, after the emerge of DSA-2018, the journalists, right bodies, civil society members from home and abroad are vocal saying the new law will curb the journalistic freedom. The conflict of journalistic freedom and legal regulations are being researched for many years in the country. More or less many of them found the principles of laws not always play positive role in safeguarding free press moreover develop barriers. Analyzing the legal situation regarding press and journalism, Khan and Kaarisma (2014) found, the tradition of long colonial legacy in law formation, laws were made to curb press freedom in British era so that their corruption would not be revealed. They also argued the passing of Right to Information Act- 2009 was a positive symptom of democratizing the information and increase the accountability in information flow. The democratizing is ensuring better access to information but still state plays a large role to manipulation the media and information flow. From 2006 to 2018, the Information Communication Technology Act (ICT Act) - 2013 was used against citizen journalists, bloggers, journalists and social media users. The Reporters

1.4 Research Methodology

This study will be conducted on the basis of secondary sources such as collecting data from internet, taking some relevant sections from Acts, find out some relevant evidence from some books and Journals. We know well that there are many different ways to approach the research that fulfils the requirements of a dissertation. These may vary both within and between disciplines. It is important to consider the expectations and possibilities concerning research in our own field. So I have tried to my level best to identify the laws, policies and programs of the court regarding contempt and mass media.

1.3 Limitations of the study

This research is the most important topic *"Digital Security Act, 2018 of Bangladesh: A Study on the Press Freedom and Journalistic Investigation'"*. Nevertheless, I shall try my best level best to collect the information on the topic refer to the research paper but to prepare the research I faced various barrier concerning information. Our SU library has not well amount of books on the topic the time period is not sufficient.

Chapter 2

The Concept of Freedom of Expression as Theoretical Framework

2.1 Concept of Freedom of Expression

Rights on 1948 which ensured Freedom of Expression as a fundamental right in its Article 19. It said, regardless of frontiers, the right of opinion and expression has ensured through any kind of media without interference. (Universal Declaration of Hunan Rights, 1948) This declaration is the recognition of political, social, economic and cultural rights of human beings though it has no legal bindings. But all country who have signed in the declaration are morally warranted to protect these rights. (Australian Human Rights Commission, 2019) The First Amendment to the United States Constitution ensures that congress would not pass any kind of law which would curtail the right of freedom of expression or of the press. Though the freedom is not absolute as in some extreme cases such as child pornography, state security and obscenity the court and government agencies can interfere. [3]

2.2 Investigative Journalism

Journalism is the process of preparing reports about the events, concepts and subjects that have influences on the society and conveying the report to the general people (Deuze, 2005). It is necessary to search the self of investigative journalism in order to analyze its correlation with both the Right to Information (RTI) and Digital Security Act. Investigative journalism is the process of uncovering in-depth information, where the goalis to dig out the factual information. Here, a relentless effort is made to break-open the closed doors of the information and to open-wide the mouths kept mum. The maincharacteristic of investigative journalism is to bring the factual truth to the daylight that is of public interest but kept secret from them intentionally (Rahman, A, 2018, P. 153).

Then, investigative journalism means searching for news based on new, exceptional and objective information over a long period of investigation. It may take some years for a journalist to collect specific information for an investigative report. The opportunity to investigate a report paves the way for bringing out specific information that can

[3] Gale, J (2010). Discourse Analysis: A Research Approach for the Moment to Moment Construction of Meaning in Systematic Practice in Human System in The Journal of Therapy, Consultation and Training.

demonstrate the shortcomings presented in other media reports (Burgh, 2008). The key tool journalism uses to discover the truth is mainly investigative reporting where areporter even bets his life to collect impartial information for unmasking the truth. A long period of investigation to uncover the truth about any influential person or political figure or about terrorism is called investigative journalism (Chepesiuk, 1997). This article has defined investigative journalism as the process of digging out information freely, publishing reports based on the findings without any hindrance and getting all possible legal help where needed.

2.3 Concept of Digital Security

Digital technology is changing the way in which society is operating and the ways we live our lives. Everyday, there is new ways to work and to play, new methods of interacting with one another. As our digital footprint grows exponentially, we are forming our own online identities. Digital security is the protection of this online identity. Criminals are finding new ways to operate and steal information from digital users for their ownpersonal gain. Digital security is an all-encompassing term which includes the tools you can use to secure your identity, assets and technology in the online and mobile world. These tools you can use to protect your identity include anti-virus software, web services, biometrics and secure personal devices you carry with you everyday. Devices such as a smart card-based USB token, the SIM card in your cell phone, the secure chip in your contactless payment card or an ePassport are digital security devices because they give you the freedom to communicate, travel, shop and work using your digital identity in a way that is convenient, enjoyable and secure.[4]

2.4 Digital Security Act 2018

The Digital Security Act 2018 is a law whose basis is mainly the previous ICT Act. Some sections of the ICT Act are amended and passed as the Digital Security Act. This newly launched law has different provisions to ensure the protection of people from offences while using digital medium or internet and to punish the offenders involved in crimes related to such medium. The initiative to enact such type of law was taken mainly to

[4] [https://www.justaskgemalto.com/en/what-is-digital-security/ last visited on 30th November, 2022].

ensure national digital security and to detect, redress, abate, prevent, investigate and try the offences related to digital medium (Draft Digital Security Act 2016). Although the initiative was taken in 2016, the law saw the formal approval from the cabinet division in 2018 after much discussions and reviews at different times and stages. The DigitalSecurity Act 2018 was approved as a new law to redress the controversies arisen surrounding the ICT Act 2006 and its amended version (2013). The law has 45 sections that discuss in detail the various types of arrangements of information and communicationsystem.

2. Investigative Journalism

The necessity of investigative journalism is enormous in terms of uncovering the objective information. There is no alternative to the investigative reporting when the question is to unmask a profound mystery related to a story by searching in-depth information and publishing report based on that. It is the common practice of all includinggovernment, corporate company, agency and even individual person to hide some decisions where hurting interests of others are related. If any person or agency wants to hide such information and any journalist presents it to the public as a report after a long investigation with an inquisitive mind, this can be regarded as investigative journalism. vulnerable, disable and other people of the society. There are various irregularities in implementing these schemes. Though, a few reports to come in the media to mention. Theland issue is another big area for investigative journalism. There are many Khas land and landless people. But, there are irregularities in allocating the Khas land. If the journalists bring investigative report on these issues regularly, good governance will be established ensuring transparency and accountability of the public administration. In this regard, a democratic environment or atmosphere is needed urgently.[5]

It is the common tendency of the people to know the up-to-the-minute information about their social structure, social system and surrounding life-reality. To know and to get information is equivalent to the fundamental right of people (Ferdous, R and Rahman, A, 2008). Every person has the right to know all the decisions and information that may have effects on their lives. On the other hand, the ruling people want to keep such information secret as they may have a mixed fear about the mixed reaction from the

[5] Bangla, BBC. (29 January 2018). Bangladesher notun Digital Nirapotta Ain 57 Dharar Bitorkito ICT Ain Theke kotota Alada?. Retrieved Ryb 18, 2018, from https://www.bbc.com/bengali/news-4286031

people. In this scenario, the journalists start a relentless effort to search for news with their inquisitive minds aiming to uncover the real truth. In this way, the necessity of reports based on investigation becomes apparent to satisfy the hunger of people to know. Abusing the power, be it political or financial, has become a common tendency for the people. In most of the cases, it is the powerful persons who involve in illegal activities including theft, killing, looting and hooliganism. Against this backdrop, removing all forms of irregularities, corruptions and arbitrariness with the ultimate goals of establishing transparency in governance is possible only if investigative journalism on right track. Such type of journalism is also essential to reduce the cases of human rights abuse and to hold the state responsible for different types of power abuse (Hossain, A, 2020).

The principal aim of investigative journalism is to uncover the truths and make them public. An investigative reporter works for months, even for years to investigate and research any specific issue deeply in order to make an investigative report that is of public interest. Whenever or wherever corruptions, conflicts and administrative irregularities are rampant, the necessity of investigative reporting is then a reality.

On the other hand, one of the main duties of the journalism professionals is to report to the public about the various sides of power abuse of powerful people for the public interests. Besides this, the journalists create mass awareness among the society by reporting on the corruption in the activities of different offices. It is also the duty of the journalists to report on whether the politicians work according to their election manifestoes made while on election campaigns. All these present the immense necessitiesof investigative journalism.

Overall, the journalists have lots of scopes to make investigative reports if they keep a kin eye on their surroundings. For example, you can see the recent corona virus issue. The main cause of spreading the virus in our country was negligence and favoritisms of some immoral personals of the airport who released expatriates taking bribes. This kind of news has come in the media very little. Here, there was scope to make investigative reports on how they passed the airport without corona virus screening. Moreover, a boy from Narayanganj or Gazipur the first corona red spot of the country went Barguna by riding a bicycle. The media cannot make an investigative report talking with the man how he could come out Dhaka and passed a long path avoiding a lot of checkpoints of law enforces team. Besides, in normal times, the journalists have a lot of fields to make

investigate reports like-the governments have many beneficiaries and social security programs/schemes for the poor.[6]

2.5 Computers and the Internet

Internet security involves the protection of a computer's internet account and files from intrusion by an outside user. Internet users today are familiar with companies like Symantec (Norton Anti-Virus) and McAfee that provide them with internet securityproducts to guard against computer viruses, as well as to provide secure firewalls and protection against spyware. Organizations like the Center for Internet Security (CIS) provide enterprises with resources for measuring information security status and making rational security investment decisions.

An example of secure smart card technology usage is the Microsoft .NET card framework. This is a software framework that is available with several Microsoft Windows operating systems. It includes a library of coded solutions to prevent common programming problems and a virtual machine that manages the execution of programs written specifically for the framework.

[6] Bangla, BBC. (2018). What are the contents inside the proposed Digital Security Act? London, BBC Bangla: Retrieved Ryb 18, 2018, from https://www.bbc.com/bengali/news-43819224

Chapter 3

IMPACT OF DIGITAL SECURITY ACT IN BANGLADESH: FEARS AND PROTECTIONS

3.1 Investigative Reporting on Government and Its Activities

An investigative journalist prepares reports based on findings of long efforts that dig out A-to-Zs of criminal activities at field level. The government offices stand top on the journalist's list of such investigations. The importance of the investigative report is immense in terms of determining transparency in activities of government offices from top to bottom levels. The politicians and government servants are sometimes convicted in various types of corruption allegations. Sometimes they took some decisions to favor the interests of different foreign donor organizations affecting the local citizens negatively. Most of the time, such decisions are kept secret. Again, some divisions of the policymakers may create a disaster for the environment. Moreover, politicians and government officials do not pay heed to the peoples' right to know information while taking decisions secretly. Nevertheless, the right to information for all is ensured by the legal framework (RTI Act, 2009). So, activities related to investigative journalism is conducted with the aim of making public all the decisions taken by the government.

3.2 Investigative Journalism in Corporate Sectors

The role of corporate sectors to the state economy is increasing remarkably. The level of corruptions in different segments of the companies is reaching to the unbearable stages too. Some of the big examples include Hallmark Scandal and Bank Forgery (Prothom Alo, 2017). In this scenario, the companies also want to keep their information secret. To cope with the competitive market, sometimes they take some decisions that go against thepublic interests. Moreover, some decisions are taken to serve personal benefits that go against the interests of the common people or the state itself. To mention, as the corporatesectors are a part of the state, it is the common people who are supplying the core capital for their businesses. So, the people do have right to know the decisions taken by the companies. To apply this right, it is necessary to conduct investigative journalism in corporate activities.

3.3 The Impacts and Fear of Digital Security Act on Investigative Journalism

The impact of the Digital Security Act 2018 on Investigative Journalism is extremely negative, as feared by many. The law has seven chapters containing a total of 45 sections. Some of the sections are surely making dangerous threats to the practices of investigative journalism. However, a few of them are acting as a safeguard for our digital devices and medium based communication systems. Overall, the fear regarding some clauses of the law is much more severe than the advantages some other provisions promise to give (Zaman, M, 2018). The preamble of the Act says that The Act is enacted to ensure National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters whereas it is expedient andnecessary to formulate an Act for ensuring National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters. But the data analysis shows that the experts see the negative impacts of the law are much more evident. The Right to Information (RTI) Act is destined to play an important role in investigative journalism. However, the new law, the government passed in the name of digital security, has included some notorious provisions that harmed the goodwill of the previous RTIAct. In fact, the Digital Security Act clashed not only with the spirit of the RTI but also with the basic civil rights and freedom of expression of the common people (Hossain, M, 2020).

The Digital Security Act will squeeze the freedom of the press as some of the sections are nothing but the alternative forms of section 57 of the previous ICT Act 2006 that invoked much controversy. As for instance, section 32 of the Digital Security Act says: *"(1) If any person commits or aids and abets in committing an offence under Official Secrets Act, 1923 (Act No XIX of 1923) through computer, digital device, computer network, digital network or through any other digital medium then he will be punished to a term of imprisonment not exceeding 14(fourteen) years or with fine not exceeding Tk.25(Twenty Five) Lac or with both. (2) If any person commits the offence mentioned in sub- section (1) for the second time or recurrently commits it, he will be punished with life imprisonment or with fine not exceeding Tk.1(one) crore or with both".*

In investigative reporting, journalists must work keeping their identities secret for uncovering the truth about the crimes/corruptions of influential people or institutions. Journalists may

face several problems if they go to collect such information and tell that they are journalists. First of all, the intended information will not come out as expected. Secondly, it may pose a dangerous threat to the life of the journalist involved. Thirdly, they may experience the real danger of physical assault or even be killed. Apart from that, the journalist might be tempted in various ways and kept away from achieving the main information or the real truth behind the event. To

avoid such obstacles and dangers, journalists use some strategies like keeping identity secret, recording conversations secretly, hiding the real purpose when they collect such types of information. Apparently, it may look like such practices go wrong with the ethics and standards of journalism. But the basic principle of journalism is to work for uncovering the truth with wider national interests in mind. So sometimes it becomes essential for them to ignore the traditional ethics to collect information of wider interests. The ground here is that if we stick to the ethics then there is a risk to cause severe damageto the country, society and people. So, journalists use the secret ways to collect such information. However, it would become impossible for a journalist to unmask the truth asusing these ways are prohibited and considered punishable crimes under the Digital Security Act. The harmful effects of these barriers would eventually fall on the shoulder of the state itself (Zaman, M, 2018).

The principal aim of journalism is to prepare and present news for the betterment of the society, state and people (Rahman, A, 2017). In doing so, a journalist can be humiliated in different ways. Taking this risk into account, the journalist must collect information without disclosing his identity with the aim of wider interest. It can be appeared as contradictory to the ethics of journalism. But considering the importance of the output, such initiatives will be considered as the big ethic. That is to say, journalists should have the freedom to use different strategies for collecting information that have wider benefits for the society (Zaman, M, 2018). But the punishments and penalties, this law does have, will demoralize the journalists to keep themselves away from collecting information vital for investigative report. For example, 14 sections, out of 20, are non-bailable. And the minimum and maximum jail terms under the law are one year and lifetime respectively while most of the offences carry imprisonment of 4-7 years which can be treated as a major punishment for a minor crime. The risky nature of the law for investigative journalism is also apparent from the protest by the Editor's Council who has put objection especially on the articles 8, 21, 25, 28, 29, 31, 32, 43 and 53 of this Digital Security Act

(Hossain, A, 2020).

So, there is a concrete ground to think that the Digital Security Act has squeezed the freedom of expression in the media. It has 48 sections in total. Of them, 17 to 48 tell about the punishments of different acts defined crime under this law. The most dangerous section 32 has provisioned the data collection process by digital devices as espionage and the punishment for such acts ranges from the imprisonment of 14 years/ a fine of 20 lac taka or both. The reality is that technology has nowadays become a tool for changing the society by dint of free flow of information. At this moment, it is the right of the citizen to know the information that affects them, and the responsibility of the journalists is to make that information public. But sometimes journalists cannot perform these professional duties due to some obstacles. Now the number one barrier is the Digital Security Act. In fact, we had forwarded our steps of independent journalism to some extent with the help of RTI Act. But this Digital Security Act has forced us to step backwards (Hossain, M, 2020).

The Digital Security Act is feared to hinder the way of flourishing democracy in the country as one of the most important elements for the democratic boom is press freedom (Zaman, M, 2018). Quoting prominent journalist North Cliff, he said that news is what somebody somewhere wants to suppress; all the rest is advertising. Searching out the news suppressed by others is the duty of the journalists. But in doing so, they are feelinga barrier due to the Digital Security Act. To mention, the main objective of journalism is to search out anyone's that information that were supposed to utter by him publicly but didn't. If such efforts are barricaded, then the investigative journalism will see its demise and “He said-She said Journalism” will be expanded (Zaman, M, 2018). Moreover,freedom of expressing the opinion and ensuring transparency and accountability are among the main conditions of democracy. Some sections of the Digital Security Act arein most cases contradictory to those conditions, hindering the democracy eventually (Ferdous, R, 2018).

To discover the truth, journalists must use some undisclosed medium in many cases (Zaman, M, 2018). Referring the Watergate Scandal, Zaman mentioned that it was not possible to make that scandal public without the use of such an option. The Watergate scandal of 1972 was a major federal political scandal in the United States involving the administration of President Richard Nixon. Washington Post reporters Bob Woodward and Carl Bernstein uncovered the scandal using devices that secretly recorded conversations. Eventually, Richard Nixon was forced to step down from the post of

President. Regarding this event as a fruit of investigative journalism, Zaman opined that journalists will fail to uncover some news of public interests like that if they are barred from using the secret medium for collecting pieces of evidence due to the Digital Security Act.

3.4. The Fields of Protection by the Digital Security Act

Many countries of the world applying this kind of act for ensuring the security of transmitting personal and organizational information through digital devices and the internet. But the reality of our country is that the act has been applying for harassment of the public; especially the journalists have become victims of the act (Siddiqui, A, 2020).

The initiative to enact the Digital Security Act was taken mainly to ensure national digital security and to detect, redress, abate, prevent, investigate and try the offences related to digital medium (Digital Security Act 2016). This law has provisions to punish the cybercriminals with different sentences based on the crime levels, which is formulated mainly to ensure personal data of people in digital medium (Ittefaq, 2018). Moreover, we have seen an incredible advance in technology-based communications forcing the decision-makers of the country to think about drafting such legislation. This isbecause the use of ICT nowadays has entered into almost every field triggering the doomsday for the old manual system of file keeping. So the government took initiatives to formulate the Digital Security Act with the aim of providing protections for the people as they enter into the new system of communication through digital medium (Salam, S A,2018).

The government also took several other strategies to cope with the needs of time while ensuring the free flow and fair use of information, addressing the misuse, utilizing them for the wellbeing of people and putting the number of cyber risks down to the zero. The country has enacted several laws to address the needs of ICT users and to make awareness among the common people as well. The final approval of the 2016‟s drafted Digital Security Act in 2018 is nothing but a sequence to that policy with the real goal isto defuse the cyber-crimes (Salam, S A, 2018). Moreover, the news media is increasingly becoming ICT-dependent triggering a need to provide the media workers with legal protection to manage them and to act with responsibilities. For instance, Bangladesh sawa manifold use of websites and digital devices due to the rapid expansion of the internet inthe country. Recently, the country connected itself to the superhighway of information through the Optical Fiber Network called South East Asia–Middle East–Western Europe

5 (SEA-ME-WE-5). On top of that, the number of internet users increased surprisingly as the country entered into the era of fourth generation mobile internet. Now over 8 crore citizens use the internet pushing the government-declared vision of Digital Bangladesh to the doorsteps of reality. Over one crore Bangladeshi citizens, now living as expatriate communities all over the world, read online-based Bengali newspapers. Given this enormous use of digital devices, it was essential to formulate some policies to address the security concerns relating to them and the Digital Security Act is the ultimate outcome from that concerns (Salam, S A, 2018).

Section 3 of the Digital Security Act says this law will get supremacy if any confrontational situation arises with other functioning laws. Apart from that, section 5 has called for forming a digital security council under the ICT division in order to ensure national digital security. Under this agency, there will be a specialized unit named Bangladesh Computer Emergency Response Team Bangladesh (CERT) to oversee all the cyber security concerns making coordinate efforts
with all other institutions. This unit will initiate prompt responses to redress any cyber-attack or such attempts (Digital Security Act 2018).

The aim of the Digital Security Council is to become a pathfinder in addressing all the problems relating to the technology-based communication and the use of digitaldevices. This council will act as the highest council body for cyber security and will provide advice and directions to the ICT division and its other subordinate institutions (Digital Security Act 2018).

The law provides assurance for the protection of private and institutionalinformation. Under section 10 of the law, a maximum five years imprisonment can be sentenced for scams related to computer, mobile and other digital devices. This cansecure the users of such digital devices from untoward situations. Moreover, appropriate punishment is ensured if any incidence of cheating or threatening occurs through digital medium (Digital Security Act 2018).

The Digital Security Act ensures harsh punishment for any person who runs any propaganda or assists in doing so against the liberation war of Bangladesh or recognition of the liberation war. The same penalty is applicable for persons propagating through online/digital medium against the Father of the Nation. So, this law initiates necessary measures to protect the country's' liberation war and related other events from propaganda (Digital Security Act 2018). This law is reducing the risk of using the free flow of information as a tool by an individual of a group to propagate their agenda. People will

also become more careful while using digital devices and they will be discouraged to disseminate information or any pictures that may defame others (Hossain, A, 2020).The law also does have measures to protect religious sentiments or values. Such as, section 28 says that publishing or broadcasting anything by means of any website or any electronic format which hurts religious sentiment or values will be considered a punishable offence (Section 28, Digital Security Act 2018). Digital Security Act 2018 also has a punishment mechanism for the offenders who intentionally publish or broadcast any kind of file in any website or digital format which creates hostility, hatred or adversity among people or destroy any communal harmony or create unrest or disorder or deteriorates or threatens to deteriorate the law and order. Such activities can be penalized with imprisonment for a term not exceeding 7 years or fine not exceeding Tk. 5 lacs or with both (Section 31, Digital Security Act). This can provide the country with a protection from different kinds of propaganda. Also, it will help spread the spirit of secularism and maintain religious coherence (Hossain, M, 2020). Moreover, this law can provide protection for the network service providers. According to the law, the service providers cannot be convicted for the offences done by their users. So, they got a scope to work independently under the protective umbrella of Digital Security Act. Apart from that, the private information of persons indicted under the law also gets privacy protection. As per the law, such information cannot be used for other purposes rather than in investigation activities(Digital Security Act). There are some people who hack other‟s digital devices with the ill-motives of gaining personal or group advantages. This law has come into effect with a harsh warning for such types of culprits. And the would-be victims will now use their electronics devices with a relief in their minds that there is a mechanism in place to get proper justice if hacked by criminals (Hossain, A, 2020). The law has a framework to settle any legal process within a very limited time. So, the law is expected to reduce the burden of the long queue of litigation providing final judgments to the people within the timeframe of the highest 180 days from the date of the lawsuit. Overall, the Digital Security Act mainly protects cyber-bullying. The adolescent group falls in internet bullying. Besides, the law checks spreading unnecessary irritation in social media. It also checks to leak various important and security-related information of the state (Siddiqui,A, 2020).

Chapter 4

SUBSTANCE AND FEATURES OF DIGITAL SECURITY ACT, 2018

4.1 Enactment of the Act

Bangladesh is an independent country having a written constitution which ensures freedom of speech in Bangladesh. The recent legislation of the Govt. has been under severe criticism as it has adopted the Information Communication and Technology Act, 2006[7] on the ground that it violates the freedom of speech. As a result, the Govt. has made a draft copy of the Digital Security Act, 2018[8] to ensure the Constitutional mandate of the country. The draft of the Digital Security Act, 2018 has been approved by the Cabinet at 29th January, 2018. It has been finally passed on September 19, 2018 by the parliament.[9]

4.2 Objects of the Act.

The bill was passed with several minor changes as recommended by the parliamentary body Section 3 of the new law includes a provision of the Right to Information Act 2009, which will be applicable in case of right to information person commits any crime or assists anyone in committing crimes under Official Secrets Act 1923, through computer, digital device, computer network, digital network or any other electronic medium, he or she may face a maximum 14 years in jail or a fine of Tk 25 lack or both. The law also includes a definition Sprit of Liberation war in section 21 which says,[1] "The high ideals of nationalism, socialism, democracy and secularism, which inspired our heroic people to dedicate themselves to, and our brave martyrs to sacrifice their lives in, the national liberation struggle According to section 29 of the law, a person may face up to three years in jail or a fine of Tk 5 lakh or both if he or she commits the offences stipulated in section 499 of the Penal Code through a website or in electronic form Section 31 of the act says a person may face up to seven years in prison or Tk 5 lack in fine or both if he or she is found to have deliberately published or broadcast something on a website or in electronic

---

7 *Information Communication and Technology Act,* 2006

8 *Digital Security Act,* 2018

9 Zulfiquar Ahmed, *A Text Book on Cyber Law in Bangladesh*, 1st ed., (Dhaka: National Law Book Company, 2009), pp.63 – 64.

form which can spread hatred and create enmity among different groups andcommunities, and can cause deterioration in law and order.[10]

As per section 32 of the law, if a includes a definition of the "Spritt of the Liberation War" in section 21, which f nationalism, socialism, democracy and secularism, which inspired our The act was passed without addressing journalists' concern over sections 8, 28, 29 and 31 that deal with haring religious values, disrupting public order, dishing out defaming information and causing deterioration in law and order by publishing anything on a website or in electronic form Though Mustafa told the House yesterday that section 57 of the ICT act would be repealed following the passage of the bill, controversial provisions of section 57 were included in four sections of the new law On July 4, the parliamentary committee at a meeting with Sampadak Parishad, Bangladesh FederalUnion of Journalists (BFUJ) and Association of Television Channel Owners (ATCO) placed an 11-point change to the proposed their consideration Representatives of share their opinion on the changes later, following discussions in respective forums The committee set July 16 for further discussion with the organizations on the bill But the meeting was postponed and no fresh date was announced arlier on May 22, the committeehad invited presidents and general secretaries of the Sampadak Panishad and BFUJ, and president and senior vice president of ATCO to a meeting to hear their views .At the meeting, the three organizations voiced concen over sections &, 21, 25, 28, 29, 31,32, and43, saying these would greatly hamper freedom of speech and independent journalism.

Digital Security Act for the three organizations told the committee that they would Earlier on several occasions, Law Minister Anisul Hug and Mustafa Jabbar assured journalists of taking measures to mitigate their concern On April 9, the Digital Secant Bill 2018 was placed in the House, which sent it to the parliamentary committee for scrutiny The committee was given four weeks to place its report before parliament Later, parliament extended the deadline for submitting the report by three months in two phases.[11]

---

10 R. K. Chaubey, *ibid*, p.143.

11 [http://www.theindependentbd.com/printversion/details/135193, last visited on 29 January, 2022].

4.3 Main features of this Act

The Act has nine chapters and 62 sections which deal with different sectors of digital security. The preamble of the Act clearly describes the purpose of the Act. In the preamble it is stated that the Act has been enacted to ensure the digital security and to identify, prohibit, suppress the offences of digitally committed crimes.

The first chapter is the introductory chapter that contains four sections (ss. 1-4). Section-2 provides definitions of different terms Section-2(2) of the Act prescribes that the definitions of the ICT Act 2006 should be taken as appropriate definitions for any term undefined in this Act.[12]

The second chapter contains three sections (ss. 5-7) which provide for 'digital security agency'. Section-6 deals with the appointment of the Director General and other Directors and their terms of office.

The third chapter contains four sections (ss. 8-11) dealing with preventive measures. Section-8 invests the Director General and the law enforcing agencies with the power to remove or block any data or information. Section-9 provides for the establishment of an emergency response team. Section-10 provides for the establishment of a digital forensic lab.

Chapter four containing three sections (ss. 12-14) deals with the digital security council. Section-12 provides for the establishment of a 'Digital Security Council' containing 13 members-

1. Chairman,
2. Minister, Minister of State or Deputy Minister of Ministry of Posts, Telecommunication and Information Technology,
3. Minister, Minister of State or Deputy Minister of Ministry of Law, Justice and Parliamentary Affairs,
4. Chief Secretary of Prime Minister,
5. Governor, Bangladesh Bank,
6. Secretary, Posts and Telecommunication Department,
7. Secretary, Information Technology Department,
8. Secretary, Public Security Department,
9. Secretary, Ministry of Foreign Affairs, lO. Inspector General of Police, Bangladesh Police, 11. Chairman, BTRC,

[12] *ICT Act*, 2006

12.Director General, Directorate General of Security Intelligence, 13.Director General, Member of Secretaries.

Section-12(2) prescribes that the Prime Minister of Bangladesh shall be the ex-officio chairman of the council. Section-13 deals with the power and functions of the council.

Chapter-5 contains only two sections and deals with critical infrastructures. It is to be mentioned that the term 'critical infrastructure' is not a defined one. Section-15 stipulates that government may by notification in the official gazette describe any infrastructure as a critical infrastructure.[13]

Chapter-6 containing 22 sections (ss. 17-38) deals with offences and punishments. The list of punishments are given below:

Chapter-7 contains sixteen chapters (ss. 39-54) which deal with investigation and trial of offences under this Act.

4.4 Section 40

Prescribes limits of investigation within 60 days. If the investigating officer fails to finish the investigation within the prescribed limit he may extend the time for 15 days with the permission of his superior officer. If the investigation is not completed within the extended time, it may be extended for further 30 days with the permission of the Tribunal.

4.5 Section 41

Prescribes the powers of the investigating officer. Section-42 deals with the power of the investigating officer regarding search and seizure with warrant. Section-43 stipulates that the investigating officer may search, seize and arrest without a warrant where there is probability that the evidences may be destroyed.

4.6 Section 47

Ensures that the information given by any person to conduct an investigation shall be kept secret. If anyone violates this provision, he shall be punished with imprisonment for 2 years(max) or fine with 1 lac taka(max) or with both.

9. [https://www.mondaq.com/Technology/880248/Introduction-To-Digital-Security-Laws-In-Bangladesh, last visited on 29 January, 2022].

The Tribunal: Section-48 prescribes that, no complaint shall be taken into cognizance by the tribunal except by written report of police. The tribunal shall follow the proceedings of Sessions Judge under section-23 of the Code of Criminal Procedure so far it is consistent with this Act.

According section-2(h), the tribunal shall be the tribunal constituted under section-68 of the 'Information Communication and Technology Act 2006'. According to section-68 of the ICT Act 2006, the tribunal shall consist of a Sessions Judge or an Additional Sessions Judge.[14]

According to section-2(a) the Appellate Tribunal shall be the Cyber Appellate Tribunal constituted under section 82 of the Information Communication and Technology Act 2006. According to section-82 of the ICT Act 2006, the appellate tribunal shall consist of a chairman and two other members. An acting or retired judge of the Supreme Court shall sit as the chairman. Other two members shall be an acting or retired District Judge and a person having knowledge and experience on information technology.

4.7 Section 52

Stipulates that a trial shall be concluded within 180 days from its commencement. And if it is not concluded within the prescribed limit, the tribunal by recording the cause in writing may extend the time for further 90 days. And if the trial is not concluded within the extended time, the tribunal informing the cause to the High Court Division in writing may continue the trial.

4.8 Section 53

Prescribes the list of offences which are cognizable and billable under this Act. Fourteen offences under sections 17, 19, 21, 22, 23, 24,26, 27, 28, 30, 31, 32, 33 and 34 of this Act are made cognizable and non-baillable. Other sections including s.8(l) (b), 20, 25, 19 and 47 are made non-cognizable and billable. The offences under section 18(1) (b) are non-cognizable, bailable and compoundable. If any person commits the same offence for the second time that will be non-bailable and cognizable. Section-54 deals with the forfeiture of the properties under this Act.

[14] *ICT Act, 2006, s. 68.*

Chapter-8 deals with regional and international co-operation and prescribes that) will be applied if any international co-operation is needed.

Chapter-9 deals with miscellaneous matters. Section- 58 prescribes that notwithstanding anything contained in the 'Evidence Act 1872', any forensic evidence collected under this Act shall be used as evidence in trials.

Section-61 repeals ss. 55, 56, 57 and 66 of the ICT Act 2006 (Act No. 39 of 2006). Section-61(2) prescribes that any case under trial under the ICT Act 2006 shall be run asif such sections has not been repealed.[15]

[15] *Ibid*., p.144.

Chapter 5

PROBLEMS AND PROSPECTS OF THE ACT

5.1 Advantages of Digital Security Act

The current government of Bangladesh, led by the Bangladesh Awami League, places considerable emphasis on digital technologies to lead the development process for the nation.

This harkens back to Vision 2021, the political manifesto of that party during the 2008 National Elections. Vision 2021 promises that, by 2021, 50 years after attaining independence, Bangladesh will become a middle income country where poverty has been completely eradicated. An important part of this is "Digital Bangladesh", a digital strategy to help transform the nation into a modern economy.[16]

To concentrate on content aspects of section 8(2), we note that it is not legitimate to censor content simply because it hampers unity, economic activity or religious sentiment. As generally understood, these are issues about which free public debate, subject to inciting to other crimes, such as violence, should be permitted. Furthermore, as a basis forrestricting free speech, these terms are too unclear. For example, if someone posts a story about air pollution leading to a drop in tourism, does that qualify as hampering economic activity? What about a story that suggests that national resources are unduly focused on Dhaka, which may fuel discontent in other parts of the country (hampering unity)? In addition, the threshold for triggering these rules is unduly very low. While blasphemy laws are generally not appropriate as restrictions on freedom of expression under international law (see below), this is all the more so where all that is required is hampering religious sentiment, which seems to reduce the threshold to a case where someone gets upset.

5.1.1 High Number of Offences

The Digital Security Act 2018 contains 19 kinds of offences. It is to be noted that The UK Computer Misuse Act 1990 contains only five offences, the Cybercrime Convention

[16] Lutfar Rahman, "Digital Bangladesh: Dreams and reality", *The Daily Star*, (10 March 2015).

contains only five offences. It is shown on the previous paragraph that many provisions of the Digital Security Act 2018 are unnecessary.[17]

5.1.2 Disproportionate Sanctions

The punishments provided in the Act are unduly harsh. Moreover, most of the offences do not articulate a significant *mensrea* requirement of 'dishonest' intent or the need for 'serious' harm which are essential to provoke a criminal punishment.

5.1.3 Exclusive Police Powers

The Digital Security Act 2018 provides police excessive powers which can prejudice the valid interests of the citizens of Bangladesh.

5.2 Bangladesh parliament passes draconian Digital Security Act

On September 19, Telecommunication and Information Communication minister Mustafa Jabbar placed the bill for immediate passage and the 350-member parliament passed the bill by voice votes with only 11 lawmakers opposing the bill. The formulation of the law was initiated in 2015 with the cabinet approving the draft on January 29, 2018 andplacing in the House on April 9, 2018.

The Editors‟ Council on September 16 in a statement rejected the bill stating that Sections 8, 21, 25, 28, 29, 31, 32 and 43 of the bill posed serious threats to freedom of expression and media.

Section 8 includes provisions about blocking or removing any information in the digital media over any content deemed hampering harmony, public order, or creating communal hatred, among other things. Section 21 states anyone „spreading negative propaganda against the Liberation War or the Father of the Nation, National Anthem and national flag‟ using digital devices or instigating to do so would be punished with imprisonment for up to life term.

According to Section 25, a person may be jailed up to five years for „deliberately publishing or broadcast on a website something attacking or intimidating or which can make someone feel disgruntled or knowingly publishing or broadcasting false or distorted information. Section 28states if anyone hurts religious sentiments, they may face jail up to 10 years. Section 29 states a person may face up to three years if they defame someone

[17] *The UK Computer Misuse Act,* 1990

as stipulated in section 499 of the Penal Code through a website. Section 31 states a person may face up to seven years in prison if they are found to have deliberately published or broadcast something on a website which can spread hatred and createenmity. Section 21, 28, 31 and 32 are classified as non-bailable offenses.[18]

5.3 New Digital Security Act imposes dangerous restrictions on freedom of expression

The new Digital Security Act under section 43 allows police in Bangladesh to arrest an individual if they believe that an offence under the law has been or is being committed or there is a possibility of committing crimes or destroying evidence. The law allows for up to 10 years imprisonment for spreading propaganda against Bangladesh's Liberation War, the national anthem and national flag using digital devices. Repeated offences carry the maximum penalty of life imprisonment.

The proposed Digital Security Act was first presented to the parliament in April 2018. In May, Bangladesh Minister of Law, Justice and Parliamentary Affairs said that the proposed Digital Security Act would be revised in consultation with the journalist community after it drew massive criticism for suppressing the right to freedom of expression and press freedoms.

The Editors Council on 17 September 2018 rejected the draft Digital Security Act as it did not make the changes that were recommended in eight sections of the law. The law fails to uphold the guarantees of freedom of expression and freedom of the press in the Constitution of Bangladesh in Articles 39(2) A and B and international treaties ratified by the country.

In early 2018 the Bangladesh government promised to repeal the draconian Information and Technology Act, in particular section 57, which was used for cracking down on freedom of expression in the country. Instead of repealing this law, the new Digital Security Act expands and reinforces the draconian Section 57 of the Information and Communication Technology Act.[19]

---

18 [https://www.article19.org/resources/bangladesh-analysis-of-the-digital-security-act,last visited on 01st February, 2022].

19 *Digital Security Act, 2018, s.57.*

Responding to the newly enacted Digital Security Act 2018 in Bangladesh which has drawn serious concerns for press freedom and the right to freedom of expression, Amnesty International's South Asia Campaigner, Saad Hammadi, said:

"This law imposes dangerous restrictions on freedom of expression. Instead of learning from the lessons of the past, it seeks to repeat them. Given how the authorities have arbitrarily arrested hundreds of people in the past six years under the Information and Communication Technology Act, there are serious concerns that the new Act will be used against people who speak out."

"The government's disregard for editors' recommendations and the concerns of the general public shows lack of concern for the grave issues regarding the bill that have been raised by civil society. The government must revert its course from this regressive law, that compromises its international commitments; and ensure they fully uphold the right to freedom of expression as protected by international human rights law."

5.3.1 Lack of Procedural Safeguards for Human Rights Protection

It is to be mentioned that the 'public interest defence' is entirely absent in the Act.

Principle-5 of the Johannesburg Principles on National Security, Freedom-.

Of Expression and Access to Information stipulates that-

'No one may be subjected to any sort of restraint, disadvantage or sanction because of his or her opinions or beliefs.'[20]

Principle-6 provides grounds where threat to national security can be punished. These are:

(a) The expression is intended to incite imminent violence;

(b) It is likely to incite such violence; and

(c) There is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.

Principle-15 provides for general rule on disclosure of secret information.

According to this principle-No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or

(2) the public interest in knowing the information outweighs the harm from disclosure.

Principle-16 provides rule for information obtained through public service.

[20] UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III),

According to this principle-No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.[21]

The Digital Security Act 2018 clearly undermines the international conventions.

[21] *Ibid*, p.144.

Chapter 6
RECOMMENDATIONS AND CONCLUSION

6.1 Recommendations

From the above discussion this thesis suggests following recommendations,

Firstly, the whole of the bill should be reviewed and edited so that its definitions and terms are as clear, practices and narrow as possible, especially where they serve as the basis for offences or the grant of power to a regulatory body.

Secondly, Rules should be reserved for matters which are properly subordinator the main legislation, rather than leaving important matters such as primary powers and responsibilities of administrative agencies and how these powers are to be exercised to the rules.

Thirdly, Section 8 (2) should not be applied at the request of law enforcement agencies. in stead only be an independent to over sight body such as the courts

Fourthly, The references to unity, economic activity and religious sentiment should be removed from section 8 (2), while a higher standard such as posing a serious risk of substantial harm of inciting should be applied to the other protected interests such as national security.

Fifthly, Section 31 should either be removed or the language should be narrowed in line with the comments above and the sanctions should be brought into line with their counterparts in the Penal code.

Sixthly, Section 38 should be amended to provide simply that service providers are not responsible for content as long as they have not intervened in the content or been ordered by a court to remove it. At minimum, the burden should rest rest on the party bringing a criminal prosecution against a service provider to show that they were aware ofthe offence.

Seventhly, Sections 22-24 should be removed. The provisions on forgery, fraud and fraudulent impersonation in the Penal Code should be reviewed and, if they fail to cover the commission of these crimes online, they should be amended to address that lacunae.

Eighthly, Sections 17(1)(a) and 18(1)(a) should either be removed (with the types of harm in section 18(1)(b) being expanded) or have intent and harm requirements added.

Ninthly, Section 32 should be limited in scope to those who are under a primary obligation to respect government confidentiality (i.e. normally officials) and those who

directly, illegally and intentionally access it, and it should also include a public interest override to protect whistleblowers.

Tenthly, An intent requirement should be added to section 33 and it should include protection for whistleblowers.

6.2 The Cyber Security Bill 2023

The Cyber Security Bill 2023 was passed in Parliament on Wednesday, keeping offences under four of its sections non-bailable. It is proposed to replace the much-talked-about Digital Security Act, in which offences under 14 sections were non-bailable .As per the Bill, officers of the rank of police inspector are empowered to search and arrest anyone without any warrant. However, if a false case is filed, it is considered as a crime and provisions for punishment have been kept. State Minister for ICT Division Zunaid Ahmed Palak moved the Bill, and it was passed by voice vote. The four non-bailable offences are related to intrusion into key information infrastructures, damaging computers and computer systems, cyber terrorist activities, and hacking related crimes.
In the law, the offences under four sections are non-bailable.
The intrusion into important information infrastructures and others are in section-17, while damaging computers and computer systems are in section-19, cyber terrorist acts and committing such crimes are in section-27, and hacking related crimes are in section-33.
The already filed cases will run under the existing law- Digital Security Act as a provision was incorporated in the proposed law.
In the draft Cyber Security Act 2023, the offences and punishment provisions have been cited in sections 17-33.
Criticizing various clauses of the Bill, opposition party members said that freedom of thought and expression and recognition of independent media have been given in the constitution itself.
However, in various clauses of this Bill, the system of curtailing these rights recognized by the constitution has been ensured.
Several members demanded to amend the provisions of arrest and search without any warrant.
In response to these criticism, State Minister Palak said that freedom of thought and expression is recognized by the constitution, but it is not unlimited.
“Freedom does not mean violating the rights of others. Your freedom does not mean saying whatever you want. It’s not about disrespecting others,” he said.
He said that the opposition members are agreeing on the necessity of the law.
“There is no alternative to the Cyber Security Act to build a transparent, accountable and secure Smart Bangladesh.”
A new section has been added in the Bill on the offence and punishment for filing false cases and complaints.
This section provides that it shall be an offence if any person files or makes a suit or complaint under any section of this act with intent to cause injury to another person, without knowing just or lawful cause for filing the suit or complaint.
The person filing the suit or complaint in this offence and the person who filed the complaint shall be punished with the punishment prescribed for the original offence.
If any case or complaint is filed under more than one section of this act, the amount of penalty for the principal offence, which is higher among the offences mentioned in the respective section may be determined as the amount of penalty.
According to the bill, on the basis of a written complaint of a person, a tribunal can accept the complaint and try the case for the crime of filing a false case and complaint.

Section 42 of the bill empowers the police to search and arrest without warrant. In this section, sub-inspector-level officers have been replaced by inspector-level officers with the power to search and arrest without warrant. This clause was also in the Digital Security Act.
Section 8 of the bill provides power to remove and block data from digital media.
This section states that if law enforcement agencies "subject to data analysis, have reason to believe" that any data published or disseminated through digital or electronic media may affect the cohesion, economic activity, security, defence, religious, or economic activities of the country or any part of the country.
Law enforcement agencies may request the BTRC through the Director General to remove or block such data if it offends values or public order, or promotes racial hatred and hatred.
Gonoforum MP Mukabbir Khan said that this law is one of the most effective tools for suppressing dissent and free thought.
In the last 4 and a half years, it has only been used to suppress criticism about the government or the ruling party. He said that using the law journalists have been tortured the most.
“Their freedom of expression has been severely curtailed by this law. This act empowers the police to enter homes and search bodies. It has given unlimited power to seize everything in any computer network, including servers. No other law has given the police so much power.”
Jatiya Party MP Fakhrul Imam said some changes have been made in the law. But journalists said they were not satisfied.
“Freedom of speech, freedom of thought, freedom of press have been ensured in the constitution. Constitution is the basic law. Any law against freedom of speech would be unconstitutional.”
Jatiya Party MP Pir Fazlur Rahman said that the Digital Security Act was controversial for everyone. The Cyber Security Act is nothing but an amendment to it.
“This will also be a hindrance to free journalism and expression. Article 42 gives power to arrest without warrant. The Act requires ensuring special protection for journalists.”
He said that there was scope for control through the Press Council.
“Expression of opinion is a constitutional right. This law is creating barriers to freedom of expression and thought.”
He said that 27 percent of the cases under the Digital Security Act have been against journalists. In most areas, the plaintiffs are the leaders and workers of the ruling party.
Another Jatiya Party MP Shamim Haider Patwari said that this law is necessary for some technical matters. But in these cases, digital security law has been used very little.
The main case has been filed on allegations of injury to consciousness and feelings, he said.
He said that the constitution has given freedom of thought, press and speech.
“As they stand, these laws are unconstitutional. The Act kept the definition of the offence the same, with reduced sentences in some cases. This law will increase the self-censorship of the media.”
Jatiya Party MP Hafiz Uddin Ahmad said that he raised objections to Section 42 and proposed to remove all illegal sections including it.
Jatiya Party MP Mujibul Haque said that journalists write for the sake of the country.
“There was an opportunity to involve the Press Council in their affairs. Article 42 gives power to arrest anyone without warrant. There is a danger of misuse of this law.”

6.3 Conclusion

Although the perceptible aim of the Digital Security Act is to abate the crimes related to digital medium, it is vivid that the fear for using some sections of the law otherwise has logical grounds. Especially, the investigative journalism is feared to take shelter inside the cold storage being impacted negatively by the law. The Digital Security Act 2018 is regarded by some people as a landmark initiative by the government in terms of providing protection to the information and communication sector. They believe that this law has ensured some provisions to identify, prevent, redress, investigate and try differentoffences involving digital devices and medium in order to maintain national digitalsecurity of the country. This law has asked for proper initiatives to protect the private information of people when they use the internet. The Digital Security Act is predicted to reduce the feuds involving religious matters as any person found involved in propagating about religions through internet or hurting religious sentiments through posting something is considered an offender and under the law and deserves exemplary punishments. Moreover, the law has included an important section that can protect the honor of Bangabandhu Sheikh Mujibur Rahman, the founding father of the nation. Any person involved in spreading misinformation against the founding father is a serious crime and will get appropriate punishment under the law. However, the anxieties the Digital Security Act press on are far more apparent than the protections it can provide. The reality is that being enacted the RTI act, easy access to information was created for the people, especially for the journalists. A segment of general people and journalistshave been exercising the RTI Act to get information from the respective departments to make the department credible, transparent and accountable to the public. But, after enacting Digital Security Act those opportunity has been deemed obstacle. Though,among two parties in the RTI Act i.e. the given sides and receiver sides the given side is being awaked more than the receiver or demand side. Because, the given side has lots of training and demonstrations for giving demanded information by the receiver side.

Especially, the Digital Security Act in no way helpful for the investigative reporting rather it is a big barrier for such type of journalism. Some sections and sub-sections of thelaw is really a big challenge on the way to use some strategies journalists consider vitalfor collecting information. Journalists now will be discouraged to practice investigative journalism that can unmask wrongdoings of the influential‟s. Rather they will feel fearful environment considering the impact of Digital Security Act. In the long run, the state itself will be deprived of the benefits of investigative journalism, hampering the flourishment of democracy as well. So, it is advisable that the law should be amendedduly to pave the way for a positive environment for both democracy and investigative journalism.

Bibliography

Books

R. K. Chaubey, *An Introduction to Cyber Crime and Cyber Laws*, 1st ed., (Kolkata: Kamal Law House, 2009)

Zulfiquar Ahmed, *A Text Book on Cyber Law in Bangladesh*, 1st ed., (Dhaka: National Law Book Company, 2009).

Noshirvan H. Jhabvala, The Law of Torts, 3rd ed. (New Dilli: N.M. Tripathi & Co; Publisher, 1948), p.174.

Statutes

Information Communication and Technology Act, 2006

Digital Security Act, 2018

The UK Computer Misuse Act, 1990

National Cyber Security Policy (NCSP), 2013.

UN General Assembly, Universal Declaration of Human Rights, 10 December 1948, 217 A (III),

Cases

Butterfield v. Forrester, (1809),11 East 90.

News Papers

The Daily Star (26 April 2018)