Research Monograph

On

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

Research Paper submitted in partial fulfillment of the requirements
of the degree of LLM (1 year) under Sonargaon University

Submitted To:

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

Submitted by:

Md. Sayham
ID: LLM 2301028014
Batch: 28
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

Sonargaon University (SU)

Submission Date: 10th January, 2024

LETTER OF TRANSMITTAL

Date:10th January, 2024

To

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

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

Dear Madam,

This is to inform you that I have completed my research monograph - on **"Digital Security Act, 2018 of Bangladesh: A Study on the Situation of Press Freedom and Journalistic Investigation"** it has been a great learning experience for me. I would like to thank you for assigning me such a responsibility and helping me on different aspects of the research monograph, which the knowledge will help in my future professional life.

However, I shall be grateful and obliged if you kindly accept my thesis and evaluate it.

Sincerely yours,

- - - - - - - - - - - - - - - - -

Md. Sayham
ID: LLM 2301028014
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

ACKNOWLEDGEMENT

First of all, I wish to acknowledge the immeasurable grace and profound kindness of the Almighty Allah. I express my gratitude to my honorable teacher **Sharmin Jahan Runa,** Assistant Professor & Head (Acting), Department of Law Faculty of Arts and Humanities, SonargaonUniversity (SU) for giving me her valuable time and important information to complete the research. As without her proper guidance it was quite impossible for me to complete the research.

I also express my gratefulness to my parents and my family member who encouraged me all the time.

Finally, I express thanks to my friends and well-wishers.

Md. Sayham
ID: LLM 2301028014
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

DECLARATION

I, hereby, declare that unless otherwise mentioned by quotation or reference, this dissertation has been entirely and solely composed by me. I further declare that all the rules prescribed for writing the dissertation have strictly been complied with. I will be subjected to penal action to be taken by the university in case these declarations are proved to be false.

- - - - - - - - - - - - - - - - -

Md. Sayham
ID: LLM 2301028014
Department of Law
Faculty of Arts and Humanities
Sonargaon University (SU)

CERTIFICATION

This is to certify that the thesis paper on **"Digital Security Act, 2018 of Bangladesh: A Study on the Situation of Press Freedom and Journalistic Investigation"** placed to the evaluation board. It is done by **Md**. **Sayham, ID: LLM 2301028014** in partial fulfillment of the requirement for the degree of the Masters of Law. The research monograph has been carried out under my guidance and is a record of the bona fide work carried out successfully.

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

Abstract

The Digital Security Act 2018 has created some barriers for citizens' accessing information and freedom of expression, particularly for the media professionals including journalists in Bangladesh. Thus, investigative journalism is now in a state of fear for distinction. In this context, the purpose of the study is to explore various effects of this Act, as well as to focus on different directions of protection while facing fears associated with the law. Digital tools became blessing for both general mass and the journalists in Bangladesh but it also came up with different scopes of misapplication. To minimize the offences, the government approved digital security Act (DSA) 2018. However, the journalist, right workers and activities becomes vocal against some sections of the law claiming those would hinder press freedom and freedom of journalist investigation. The collected data evaluated through the theoretical framework of Freedom of Expression concept. The findings revealed: investigative journalists and other media professionals were suffering from a sense of fear; eventually they were censoring their contents which actually went against the standard of freedom of expression.

TABLE OF CONTENTS

Sl No.	Title	Page No.
Capter:01	**INTRODUCTION**	1-2
	1.1 Introduction	
	1.2 Research Methodology	
	1.3 Limitations of the study	
Chapter:02	**THE DIGITAL SECURITY ACT 2018**	3-8
	2.1 The Digital Security Act	
	2.2 Why is this Law necessary	
	2.3 Why is this law initiated	
	2.4 Digital Security Agency	
	2.5 Preventive Measures	
	2.6 Digital Security Council	
	2.7 Critical Information Infrastructure	
	2.8 Crime and Punishment	
	2.9 Investigative Journalism	
	2.10 Why Investigative Journalism	
Chapter:03	**IMPACT OF DIGITAL SECURITY ACT IN BANGLADESH: FEARS AND PROTECTIONS**	9-15
	3.1 Investigative Journalism in Corporate Sectors	
	3.2The Impacts and Fear of Digital Security Act on Investigative Journalism	
	3.3 Investigative Reporting on Government and Its Activities	
	3.4 The Fields of Protection by the Digital Security Act	
Chapter:04	**RIGHT TO PRIVACY JOURNALIST AND DIGITAL SECURITY ACT 2018**	16-20
	4.1 Preamble	
	4.2 Digital Security Agency	
	4.3 Digital Security Council	
	4.4 Bangladesh Government‘s Computer Incident Response Team	
	4.5 To achieve the goal, BGD E CIRT during the first of its	

	development will	
	4.6 Protection of Right to Privacy through Digital Security Act 2018	
Chapter 5:	**A LEGAL ANALYSIS ON DIGITAL SECURITY ACT 2018 PRESS FREEDOM AND JOURNALIST INVESTIGATION**	21-30
	5.1 The act contains the following fundamental flaws	
	5.2 The provisions of the Digital Security Act that find most dangerous	
	5.3 The Cyber Security Act 2023	
Capter-06	**CONCLUSION**	31-33
	6.1 Recommendations	
	6.2 Conclusion	
	Bibliography	33-34

Chapter 1
INTRODUCTION

1.1 Introduction

Investigative journalism is a process of digging out in-depth information. Here a relentless effort is made to open the doors of information uncovering those stories some people want to keep secret. It is such a public interest-based reporting which helpsuncover corruption and increase awareness among the citizens. This process involves the preparation and publication of reports that are based on authentic data that can promote public welfare. To uncover the factual stories kept secret from the public intentionally andto report for the betterment of the common people is investigative journalism. We can perceive what roles the investigative reporting can play to root out the corruption from theincident famously known as `Watergate Scandal'. Carl Bernstein and Bob Woodward,two young reporters from the Washington Post made a concrete example of the strength of such reporting does have. They uncovered the major federal political scandal in the United States involving the administration of President Richard Nixon. The journalists sometimes are bound to adopt new strategies to become successful in investigative reporting. As part of those strategies, they cannot collect information publicly. In doingso, they often fall prey to various kinds of risk and insecurity. For example, digitaldevices are used to collect documents, sometimes considered `info-theft'. Against this backdrop, the government enacted the Digital Security Law to ensure national digital security and to detect, redress, abate, prevent, investigate and try the offences related to the digital medium. The Law calls for to ensure the protection of the public while theyuse digital devices for communication and information exchange. It is also supposed to favor the internet-based info exchanges and protect the process from the offenders. However, journalists, human rights activists and members of civil societies are criticizing the law given the negative impacts some provisions of the law do have. Especially, investigative journalism is bound to have enormous barriers as the main strategy of such reporting is to search out alternative ways of information collection to uncover wrong doings that can affect public interests. But the Digital Security Act 2018 consider collecting information secretly an offence resulting in huge barriers to the way of investigative reporting[1].

1.2 Research Objectives

1. An overview of Concept and historical Background of Digital Security Act
2. To analyze the Digital Security Act and Investigative Journalism in Bangladesh
3. To find out the Digital Security Act- 2018 of Bangladesh; a Study on the Situation of Press Freedom and Journalistic Investigation
4. To find out the Advantage and disadvantage of the Act
5. To suggest in the concerned matters.

1.3 Research Methodology

In any research data collection is very important. Every research involves methods by which desired result can be achieved in this regard; I have following analytical method to complete this research the data from secondary sources which include different Acts Newspaper books and web sites etc.

1.4 Limitations of the study

Each research study has some limitations. So this research monograph is not exception of this limitation and reduced the scope of the study. The main limitation to prepare this thesis is time limitation. To make a fulfill thesis the time period is not sufficient. Another problem is no specific book on ‒Digital Security Act, 2018 of Bangladesh: A Study on the Pres Freedom and Journalist Investigation‖ so it is very difficult to collect materialson that topic. Though I have taken the help from various books, internet, article, journal.

[1] Digital Security Act 2018 (08 October, 2018), Legislative and Parliamentary Affiars Division,, Government of the Peoples Republic of Bangladesh

Chapter 2

THE DIGITAL SECURITY ACT 2018

2.1 The Digital Security Act

The parliament passed the Digital Security Act on 8th October 2018. This act provides digital security for any repugnant cyber-crimes committed by digital devices or computer technology.[2]

According to , section 2(I) of the Digital Security Act 2018 ,–Digital‖ means a working method based on double digit (0 and 1/binary) or digit, and, for carrying out the purposes of this Act, also includes electrical, digital, magnetic, optional, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology; According to, section 2(j) –Digital device‖ means any electronic, digital, magnetic, optical, or information processing device or system which performs logical, mathematical and memory functions by using electronic, digital, magnetic or optical impulse, and is connected with any digital or computer device system or computer network, and also includes all kinds of input, output, processing, accumulation, digital device software or communication facilities; According to section 2(k) –Digital security‖ means the security of any digital device or digital system; The new Digital Security Act 2018 is to deal with slander, hurting, religious, sentiment, abuse of law and order or organization through publishing any material on a website.

2.2 Why is this Law necessary

Personal information of an individual collected for a particular purpose is commonly misused for other purposes, like direct marketing without the consent of the individual.

---

[2] Faruque, M.O. and Habibullah, S.M., 2018. Privacy as a Human Right in the Digital Age: In Quest of a Safer Protection Regime in Bangladesh. Privacy as a Human Right in the Digital Age: In Quest of a Safer Protection Regime in Bangladesh (October 10, 2018). ELCOP Yearbook of Human Rights.

[https://www.academia.edu/41174014/THE_RIGHT_TO_PRIVACY_IN_BANGLADESH_IN_THE_CONTEXT_OF_TECHNOLOGICAL_ADVANCEMENT, last visited on 20.12.2022].

Some internal confidentiality standard within the system is required so that personal information of an individual does not get transferred to others easily causing irreparable distress or embarrassment."* So it has to be clear in the new law that personal information of an individual collected for a particular purpose should be used for that particular purpose.

Digitally occurring crime through FACEBOOK, WHATSAPP may be controlled. Fake news through journalists will be stopped by this law.

Recently, hacking incidents of databases of governmental organizations in Bangladesh are indicating the breach of personal data stored in their server. For instance, some unknown hackers breached Bangladesh Air Force's website and extracted the full database, Official website of Bangladesh Parliament in 2013 and Official website of Bangladesh Judicial Service Commission.

While Bangladesh is well protected by virtue of the Information and Communication Technology (ICT) Act, 2006 to bring proceedings against perpetrators of such intrusion and unauthorized access, what it fails to take into account is that these perpetrators carry out their operations anonymously and thus, in most cases, it is difficult to identify them.In other words, a preventive framework at the pre-breach level is simply non-existent. There is some protection ensured by various Acts and Regulation on piecemeal nature, however there is no comprehensive data protection for consumers and general public for their non-electronic data provided to various organizations, companies and corporations.[3]

2.3 Why is this law initiated

i. To deal with defamation, hurting, religious sentiments.
ii. Causing deterioration of law and order.
iii. Instigation of violence against any personal organization by publishing or transmitting any material on any website or electronic media.

[3] [https://www.justaskgemalto.com/en/what-is-digital-security/ last visited on 20 December, 2022].

2.4 Digital Security Agency

Digital Security Act 2018, under section 5, describes the formation of an agency. To fulfill the objective of this act. Forming agency notification given by the government in the official gazette shall create an agency entitled as Digital Security agency consisting of1 (one) Managing Director and 2 (two) Director. The head quarter of this agency will bein Dhaka if needed branch offices of the agency can be established in any place in the country outside of Dhaka. The responsibilities and powers of the agency will be determined in accordance with the rules. The managing director and the directors will be appointed as a full-time employee by the government. The managing director and directorwill follow the provisions of this act and the rules implemented under this act in performing functions, exercising power, performing responsibilities as directed by the government. This agency can appoint a significant number of employees with the term of employment.

2.5 Preventive Measures

The director of the Digital Security agency can request to BTRC to block or remove the information or data published, which is a threat to Digital Security .Any religious values, racism, or hatred which hampers any terms of nations, the law, and national security force can request to the BTRC via the General Director of the Agency. After notifying, BTRC can immediately remove the information or data in the subject matter of the request to the government.

Under section 9, the emergency response team will fulfill their responsibilities by-

Ensuring the security of critical information infrastructure

If there is any cyber, digital attack, or digital security is hampered, they can take necessary emergency steps to block it.

To fulfill the objectives by the permission of the government to take the overall initiatives, including information exchange with any similar international agency or organization.

The agency will coordinate activities with the emergency team and can also supervise them.

To fulfill this object of this act, there will be one or more forensic labs under the supervision of the agency. This digital forensic lab is established under government authority, and its quality requirements are under section 11 of this act. Moreover, this digital forensic lab will coordinate with the agency, and rules will determine the establishment of this lalab under the supervision of the agency. This digital forensic lab isestablished under government authority, and its quality requirements are under section 11 of this act. Moreover, this digital forensic lab will coordinate with the agency, and rules will determine the establishment of ccment, and the law became effective.

2.6 Digital Security Council

National security agency formed under section 12, with thirteen members and theirpowers explained under section 13. They can perform their abilities if the situation of digital security is under threat and provide necessary steps to remedy the situation. Also, under this power, they advise improving digital security infrastructure, manpower, and quality. More to add, they can take the necessary steps to ensure the implantation of this act. And the agency will provide the necessary support to the council to perform its duty.

2.7 Critical Information Infrastructure

Under the digital security act 2018, section 15, the government can declare through government gazette any crucial information of a computer system or network.

2.8 Crime and Punishment

If any person intentionally or knowingly enters illegally in any critical information infrastructure and harms, destroys, or tries to do so will be an offensive act because of his activity under the digital security act 2018, section 17. Committing this aggressive act by any person will be penalized by imprisonment for a term not exceeding 7(seven) years or by fine not exceeding 25(twenty-five) lacs taka or with both. Also, the intention ofharming or destroying the information, the person will be penalized by imprisonment fora term not exceeding 14 (fourteen) years or with fine not exceeding 1(one) core taka or with both.

Any person tries to make an illegal entrance in computer or digital device also has the intention to commit a crime will be offense under Digital Act 2018, section 18 sub (1) and will be penalized by imprisonment for a term not exceeding 3(three) years or by fine not exceeding 10 (ten) lacs taka or with both.[4]

2.9 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 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.

2.10 Why Investigative Journalism

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

[4] [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a- 42377844 last visited on 15h December, 2022].

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.

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 Khash 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]

[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

Chapter 3

IMPACT OF DIGITAL SECURITY ACT IN BANGLADESH: FEARS AND PROTECTIONS

3.1 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.

3.2 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 mayface 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 act 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 feeling

a 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 SecurityAct.

3.3 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.

3.4 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 Europe5 (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 digital devices. 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 orany 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 2018also 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, hatredor adversity among people or destroy any communal harmony or create unrest or disorderor 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).

Ibid, p.138

Chapter 4

RIGHT TO PRIVACY JOURNALIST AND DIGITAL SECURITY ACT 2018

4.1 Preamble

The Digital Security Act (DSA) was enacted in the year 2018 purportedly replacing the controversial Section 57 of the Information and Communication Technology Act, 2006 (as amended in 2013). 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 from people of many walks for the abolishment of the DSA. In response, the risk of unsupervised/unprotected use of cyberspace has often been presented as a justification for the legislation. In this backdrop, it is important to identify what is wrong with the Act, if any.

Bangladesh is home to 87 million internet subscribers, accounting for approximately 53% of its entire population. In 2016, Bangladesh was ranked 112 out of 139 nations on a Network Readiness Index according to a World Economic Forum report, while also performing poorly in the Global Cyber security Index in 2015. The contemporaneous legal framework, i.e. the Information Communication Technology Act of 2006, was largely held to be insufficient in terms of addressing digital security and data protection concerns. Consequently, Bangladesh has taken steps to improve its digital securityframework through its e-governance project and "Digital Bangladesh"4 vision. Further, the government formulated a National Cyber security Strategy, charting a vision for cyber-security till 2021.

Passed with the objective of curbing cybercrime and ensuring digital security, the Digital Security Act creates a wide range of cyber-crime 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 telecom regulator remove/block the same In this Act has turned out with a great impression that it protects

private data, personal information. According to section 2(26) of the Digital security Act 2018, any information which identifies a person or system or the name, date of birth, address and any kind of personal details is regarded as identity information. Fingerprint, voice print, iris image, retina image, digital signature or other identifiers which can detect a person more efficiently all include identity information.

4.2 Digital Security Agency

Digital Security Act 2018 under section 5, describes the formation of the agency to fulfill the objective of this Act. Forming agency notification given by the government in the official gazette shall create an agency entitled as Digital Security Agency consisting of 1 Managing Director and 2 Director.The headhunter of this agency will be in Dhaka if needed a branch of the agency can be established any place in the country outside in Dhaka. The responsibilities and powers of the agency will be determined in accordance with the rules . The managing director and director will follow the provisions of this Act and rules implemented under this Act in performing functions, exercising power, performing responsibilities as directed by the government.

The director of the digital security agency can request BTRC to block or remove the information or data published which is a threat to digital security. Any religious values, racism or hatred which hampers any term of nations, the law and national security force can request to the BTRC via the General Director of the agency.[6]

Under section 9, the emergency response team will fulfill their responsibilities by-

Ensuring the security of critical information infrastructure.

If there is any cyber, digital attack, or digital security is hampered, they can take necessary emergency steps to block it.

To fulfill the objective by the permission of the government to take the overallinitiative including information exchange with any similar international agency or organizations.

---

[6] [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a- 42377844 15h December, 2022].

4.3 Digital Security Council

National Security agency formed under section 12, with thirteen members and their powers explained under threat and provide necessary steps to remedy the situation The Government of Bangladesh for protecting the cyber world against security threats, risks and challenges to national security. The Strategy addresses the country's national securitystrategy. The purpose of this document is to create a coherent vision for 2021 keeping Bangladesh secure and prosperous by coordinating government, private sector, citizens and international cyberspace defense efforts.

4.4 Bangladesh Government's Computer Incident Response Team

Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) is acting as the National CIRT of Bangladesh (N-CIRT) currently with responsibilities including receiving, reviewing, and responding to computer security incidents and activities. Under the Government of People's republic of Bangladesh, BGD e-GOV CIRT reviews and takes necessary measures to resolve the issue with broad cyber security ramifications, conducts research & development and provides guidance on security vulnerabilities. BGD e-GOV CIRT also works with various government units, Critical Information Infrastructures, financial organizations, law enforcement agencies, academia & civil society to help to improve the cyber security defense of Bangladesh. BGD e-GOV CIRT has a very strong tie with international organizations and cyber security communities and is working as a focal point of Bangladesh for trans-border cyber issues.

BGD e-GOV CIRT has currently the following active service components:

i. Incident Handling Unit.
ii. Digital Forensic Unit.
iii. Cyber Awareness & Capacity Development Unit.
iv. Cyber Sensor Unit.
v. Cyber Range Unit.
vi. Cyber Risk Assessment Unit.
vii. Critical Information Infrastructure Unit.

4.5 To achieve the goal, BGD E CIRT during the first of its development will

Monitor the network for the events that affects security of the government network; Carry out investigations and containment measures for cyber security events in order to minimize data loss or service disruption in the government network and e-services; Help to solve security related issue in National Data Center (NDC) including provision of obligatory instructions for BCC personnel to secure NDC information resources;

Carry out preventive measures in order to minimize disruptions of secure operations of the government network and e-services; Participate in international and national cyber security initiatives;[7]

Promote and strengthen cyber security environment by developing, collaborating and maintaining relationships with other CIRTs and organizations in the country and abroad; Support capacity building in cyber security of the existing manpower of BCC.

4.6 Protection of Right to Privacy through Digital Security Act 2018

Cyber security acts have been enacted in many countries. Digital Security Act 2018 was such an act in Bangladesh which was established to ensure personal security and organizational information through digital devices and the internet. This act has some provisions in which there is a declared punishment for cyber criminals depending ontypes of cybercrime. Nowadays the use of ICT has become a lifestyle as it has entered into every step of our daily life. That's why the government has taken necessary steps through the Digital Security Act 2018 to protect personal information, dignity of the nation as well as people entering into the advanced communication and technologysystem through digital media.

The Digital Security Council works as a pathfinder to detect all types of cyber-related problems associated with the highest council body of cyber security and provide necessary directions and advice to the ICT division and its subordination institution. As the right to privacy is an essential need for an individual, the Digital Security Act ensures the protection of personal and institutional information. Maximum five years

[7] [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a- 42377844 last visited on 22h December, 2022].

imprisonment can be sentenced for scams related to computer, mobile and other digital devices under the section 10 of this law. In addition if any kind of threatening orharassment occurs through any kind of digital devices appropriate punishment is assured.

So this law creates a barrier for the users of the digital devices to access anyone‘s personal data or information (Digital Security Act 2018). The law also gives an emphasis on religious sentiments or values. Publishing or broadcasting anything that hurts religious values through any electronic media or websites will be treated as a punishable offence (Section 28, Digital Security Act, 2018). Also, if anyone intentionally publishes anything that creates hostility, destroys any communal harmony, creates hatred among the people then imprisonment for a term not exceeding 7 years or fine not exceeding TK. 5 lakhs or with both can be sentenced (Section 31, Digital Security Act 2018). This surely can provide a disciplined environment in any country and gives protection from various propaganda. There is a harsh punishment for those culprits who hack others' digital devices for blackmailing them and gaining advantage. So anyone can use their digital devices keeping in mind that there is a proper justice if he or she is hacked by any criminals. The digital Security Act also provides a protection from any kind of propaganda which is against the liberation war of Bangladesh. If anyone spreads anything against the liberation war of Bangladesh through any electronic device or digital device the person will be punished according to this law. The person who publishes anything against the Father of the Nation will be treated in the same way also. So, this law protects the dignity of the country's liberation war (Digital Security Act 2018).[8]

Moreover, this law also ensures protection from the network service provider. If any user does any illegal activities, the network provider will not be convicted according to this law. So establishing the Digital Security Act by the government of Bangladesh was a tremendous decision for protecting privacy of personal or institutional information. Through this act basically _right to privacy is preserved for human beings.[9]

---

[8] [https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf, last visited on 22h December, 2022]

[9] [http://www.telecomindustrydialogue.org/resources/bangladesh/, last visited on 22h December, 2022].

Chapter 5

A LEGAL ANALYSIS ON DIGITAL SECURITY ACT 2018 PRESS FREEDOM AND JOURNALIST INVESTIGATION

The Digital Security Act (DSA) just passed in parliament gives the police authority to arrest anyone without a warrant. The act has defined at least 14 offences as non-bail able**.**

5.1 The act contains the following fundamental flaws

1. In trying to make a law to prevent crimes through digital devices and provide security in the digital sphere, the act ends up policing media operations, censoring content and controlling media freedom and freedom of speech and expression as guaranteed by our constitution.

2. The act gives unlimited power to the police to enter premises, search offices, bodily search persons, seize computers and networks, servers, and everything related to the digital platforms. According to the act, the police can arrest anybody on suspicion withoutwarrant and do not need any approval of any authorities.

3. The act suffers from vagueness and uses many terms that can be misinterpreted and used against the media.[10]

4. DSA will create an atmosphere of fear and intimidation which will make journalism and especially investigative journalism virtually impossible.

5. Other than media professionals, the law will create panic among all users of computers, computer networks, etc.

When the ICT Act was made in 2006, the government said journalists had nothing to fear as its aim was to prevent cyber crimes and punish cyber criminals. The reality is journalists and people who exercised their constitutional rights to freedom of speech suffered imprisonment and harassment under Section 57 of the ICT Act. The same is nowbeing said that journalists have nothing to worry about the DSA, but the apprehension is that journalists will again face the same kind of harassment by this law.

[10] *Information Communication and Technology Act, 2006 s. 57.*

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 the problem is that DSA goes much beyond its defined scope and ventures into the territory of 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. The DSA deals with the digital world which is ever evolving. Digital technology is all pervasive from national security to food production to health services to financial transactions, and media are no exception.

While other fields mentioned above may require ‒regulations‖ , the media needs ‒freedom‖. The DSA is focused only on the ‒regulation‖ aspect and totally neglects the need for media freedom. This is one of the fundamental flaws of DSA, making it so dangerous for the media.

A frightening aspect of the DSA is the enormous arbitrary power given to the police who may arrest a journalist just on suspicion of a so-called crime that he thinks may be committed in the future. The police are allowed to make such arrests which have been made mostly non-bail-able without any warrant. In practical terms this will bring journalism under the control of the police.[11]

5.2 The provisions of the Digital Security Act that find most dangerous

(a) Section 8: Power to remove or block information and data: (1) If the director general is satisfied that something that is published or disseminated in the digital platform falling within his domain may pose as a threat to digital security, he may request Bangladesh Telecommunication Regulatory Commission (BTRC) to remove such information or data or, in specific cases block the platform.

(2) If it is evident to the law enforcing agencies that something published and disseminated through any digital device or digital medium can create disunity in the country, disrupt economic activities and security, defense, hurt religious values, create communal hatred or bad feelings, create law and order situation then the law enforcing agencies can request the BTRC to remove such content or block it.

[11] *Digital Security Act, 2018 s. 18.*

(3) On receipt of such requests, BTRC while informing the government will take immediate action to remove or block the content.[12]

The justification needed to remove or block content is too vague and subject to individual interpretation and hence leave the scope for abuse of the law. For example, if exposing corruption in a project leads to stopping its financing by any donor or a private investor, then a journalist can be accused of ―disrupting economic activity‖ under this law and this can lead to blocking or removal of the content.

(B) Section 21

Punishment for any propaganda against Liberation War, Spirit of the Liberation War, Father of the Nation, National Anthem and National Flag:

(1) If an individual generates propaganda against The Liberation War, Spirit of Liberation War, Father of the Nation, National Anthem and National Flag or assists in such a process then such action will be considered a crime.

However, when laws are being framed we need to be very clear and specific. Given its present form, not only journalists but historians, researchers and even creative writers like novelists will also suffer. It may even result in people not writing or researching much on our Liberation War fearing misinterpretation and the possibility of punishment.

(C) Section 25

Publishing or distributing attacking, false or intimidating information or data:

(1) If any person using a website or any digital device-(a) deliberately or knowingly distributes any information or data that is attacking or intimidating in nature; or if a person publishes or distributes any information despite knowing that it is false to irritate, humiliate, defame or embarrass or to discredit a person or

(b) Damages the image and reputation of the State or spreads confusion or with the same purpose publishes or distributes fully or partially distorted information or data despite

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

knowing that it is false, and if any one assists in such actions then all such actions of the individual will be considered a crime.

This will directly affect all investigative reporting in the media. Such reports are usually about some irregularities performed by institutions and individuals. Corrupt people will use this law to intimidate journalists and media organizations and try to prevent publication of such stories on the pretext that the reports have attacked or intimidated them. Actually every such report can be said to fall under one or more of the above categories and can be used to harass the media.

(D) Section 28

If any website or electronic system publishes or broadcasts anything that hurts religious values and religious sentiments etc.

(1) if any person or group deliberately and knowingly and with the intention of hurting religious values or sentiments or with the intention to provoke such sentiment publishes or broadcasts information then such actions will be considered a crime.

The term ‒religious sentiment‖ is a very undefined term. How can a reporter know how and when religious sentiment has been hurt? This term lends itself to diverse interpretations and no journalist will feel comfortable about reporting on such issues. Thiswill prevent journalistic scrutiny over a large area of the society. The recent reporting on the sexual harassment by Catholic priests would not have been possible if those countries had a law preventing reporting that ‒hurts‖ religious sentiments. Criticizing unlawful fatwa or women's property rights may be interpreted by some as ‒hurting‖ their religious values. This section can lead to widespread harassment of journalists.

(E) Section 29

Publishing and distributing defamatory information, etc.—1) If a person publishes or distributes any defamatory information mentioned in section 499 of the Penal Code (Act XLV of 1860) via a website or any other electronic format, they will get a maximum penalty of 3 years in jail or Taka 5 lakh in fine, or both. A law already exists to deal with defamation and so a separate law for digital media is not needed. Moreover, there is no logic for enhanced penalty for digital media from print media for the same crime.

(F) Section 31

Crimes and penalties for deterioration of law and order, etc. 1) If a person deliberately publishes or broadcasts via a website or any digital platform anything that creates enmity, hatred or acrimony among different classes or communities, or upsets communal harmony, or creates unrest or chaos, or causes or begins to cause deterioration in law and order, then that activity of the said person will be considered crime. A news report concerning discrimination of Dalit‘s or ethnic groups and exploitation of disadvantaged groups may be interpreted as causing disaffection between different groups. Any news highlighting plights of the people of Chittagong Hill Tracts may be interpreted as –creating unrest‖ among different communities. Similarly, news about possible labor unrest, impending hartal or demonstration can be construed as reports that are –creating law and order situation‖ and thus bring action under this law. There could be a story that a person has died in a demonstration which may later prove to be untrue. Will the media be –guilty of spreading rumors' '? Such errors regularly occur in reporting which are corrected immediately. In Bangladesh death figures from floods, cyclones or even road accidents vary. Government figures are always at variance with privately gathered figures. In such cases, according to the DSA, the media can be sued for –spreading rumors‖. Sometimes reports may forecast certain developments which may not exactly happen later. That also can be considered as –spreading rumors' '. Thus we find this section seriously jeopardizing freedom of journalism.

(G) Section 32

32) Offence and penalty for breach of Official Secrets—1) If a person commits a crime or assists someone in committing a crime under the Official Secrets Act, 1923 (Act No XIX of 1923) via a computer, digital device, computer network, digital network or any other digital media, they will get a maximum penalty of 14 years in jail or Tk 2.5 million in fines, or both.

2) If a person commits a crime mentioned in the sub-clause (1) for a second time or repeatedly, they will be sentenced to life in prison or a maximum fine of Tk 10 million, or both.[13]

[13] [http://www.theindependentbd.com/printversion/details/135193, last visited on 24h December, 2022].

This is a sweeping restrictive law from the colonial times that was promulgated to protect the British administration from any sort of accountability. It is shocking to see it being incorporated for digital platforms. Anything that is not made public by the government is deemed an ‒official secret‖. Let us take an example. We have published dozens of reports about bank defaults based on Bangladesh Bank's findings. All such reports can be said to have violated the Official Secrets Act. All government reports which have not been made public, say, on pollution or child nutrition, are a part of the Official Secrets Act. both.

(H) Section 43

43) Search, Seizure and Arrest without Warrant—1) If a police officer has a reason to believe that a crime under this law has been or is being or will be committed in any place, or there is a possibility of it happening, or if there is a possibility of evidence being lost, destroyed, deleted or altered or being made scarce in some other way, then the officer, upon putting in writing the reason for his/her belief, can undertake the following tasks:

Attack on Freedom of Expression in Bangladesh:

Article 19 of the Universal Declaration of Human Rights (UDHR) protects the right to freedom of expression. International Covenant of Civil and Political Rights (ICCPR) was ratified by Bangladesh in 2000. Thus it is legally bound to ensure its right to freedom of expression mentioned in Article 19 of ICCPR. It has been affirmed by the UN Human Rights Committee that the right includes the freedom of expressing thoughts and opinions which the other people may find derogatory. ARTICLE 19‘s analysis shows that 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 criminalize a wide range oflegitimate 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.[14]

ARTICLE 19 concludes that the 2018 Act is deeply flawed and that it should be reviewed and its most problematic provisions repealed as a matter of urge**.**

Section 52:

The judge of the Tribunal shall dispose of a case under this Act within 180 (one hundred and eighty) working days from the date on which the charge is framed. (2) If the judge of the Tribunal fails to dispose of a case within the time-limit specified in sub-section (1), he may, for reasons to be recorded in writing, extend the time-limit up to 90 (ninety) days. (3) If the judge of the Tribunal fails to dispose of a case within the time-limit specified in sub-section (2), he may, with intimation to the High Court Division in the form of a report

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

5.3 The Cyber Security Act 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, defense, 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.
Gono forum 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 has 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.”

---

15 *https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill-2023*

Chapter 6

CONCLUSION

6.1 Recommendation

Article 19 review

(i) In this analysis, Article 19 reviews the compatibility of the Bangladesh Digital Security Act 2018 (the 2018 Act), adopted in October 2018, for its compliance with international standards on freedom of expression.

Right to freedom of expression

(ii) Analysis is based on Bangladesh's obligations under international human rights standards, in particular those on the right to freedom of expression, as they apply to the domestic guarantees to freedom of expression in the Bangladesh Constitution.

(iii) This analysis not only examines human rights concerns with specific sections of the 2018 Act, but also offers concrete recommendations on how each section discussed below may be modified to ensure their compatibility with international standards.

Article 19's

(iv) Unfortunately, Article 19's analysis shows that 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:

(v) The Act vests sweeping blocking powers in a government agency.

(vi) It contains several speech offences, including criminal defamation, defamation of religions, or the sending of offensive information that would criminalize a wide range of legitimate expression.

(vii) 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.

(viii) Article 19 concludes that the 2018 Act is deeply flawed and that it should be reviewed and its most problematic provisions repealed as a matter of urge.

6.2 Conclusion

The Digital Security Act 2018 is considered as a prominent step by the government of Bangladesh to protect the privacy related things or information of an individual or organization from the free flow of the internet. This law also ensures protection from the network service provider. If any user does any illegal activities, the network provider will not be convicted according to this law. So establishing the Digital Security Act by the government of Bangladesh was a tremendous decision for protecting privacy of the personal. The main aim of enacting this act is to reduce cybercrime activities by using digital devices. It also reduces the feuds which are involved with religious matters. Spreading misinformation about the founder of the nation is treated as a serious crime under this law. To ensure privacy through this act the hacking activities are strictly banned and the person who will do such type of activities will be punished with institutional information. Through this act basically right to privacy is preserved for human beings.

Bibliography

Books

1. R. K. Chaubey, *An Introduction to Cyber Crime and Cyber Laws*, 1st ed., (Kolkata: Kamal Law House, 2009)
2. Zulfiquar Ahmed, *A Text Book on Cyber Law in Bangladesh*, 1st ed., (Dhaka: National Law Book Company, 2009).
3. Noshirvan H. Jhabvala, *The Law of Torts*, 3rd ed. (New Dilli: N.M. Tripathi & Co; Publisher, 1948).

Statutes

1. *Information Communication and Technology Act,* 2006
2. *Digital Security Act,* 2018
3. *The UK Computer Misuse Act,* 1990
4. *National Cyber Security Policy (NCSP),* 2013.
5. *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III),

Cases

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

News Papers

1. *The Daily Star*

Website

1. https://www.justaskgemalto.com/en/what-is-digital-security/].
2. [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a-42377844].
3. [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a-42377844].
4. [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a-42377844].
5. [https://www.dw.com/en/bangladeshs-new-digital-security-law-alarms-journalists/a-42377844].
6. [http://www.theindependentbd.com/printversion/details/135193].

7. [https://www.mondaq.com/Technology/880248/Introduction-To-Digital-Security-Laws-In-Bangladesh].
8. [https://www.mondaq.com/Technology/880248/Introduction-To-Digital-Security-Laws-In-Bangladesh].
9. [https://www.article19.org/resources/bangladesh-analysis-of-the-digital-security-act].
10. [http://progressbangladesh.com/anonymous-hacks-police-and-rab-websites/].
11. [http://www.bankinfosecurity.com/report-bangladesh-probes-2013-bank-hack-via-swift-a-].
12. [http://www.straitstimes.com/business/dridex-malware-linked-to-bangladesh-heist].
13. [https://www.dhakatribune.com/bangladesh/325228/parliament-passes-cyber-security-bill-2023]