EAST WEST UNIVERSITY

SUPERVISED DISSERTATION

ON

Cyber Defamation in Bangladesh: Evaluating the Legal Regime of Bangladesh through the Lens of International Law Perspective

Course Title: Supervised Dissertation

Course Code: Law 406

Submitted To

Md. Pizuar Hossain
Senior Lecturer
Department of Law
East West University

Submitted By

Rakibul Hasan Mugdho
ID: 2019-1-66-035
Semester: Spring 2023

Word Count: 7311

Date of submission: 21.05.2023

The dissertation titled “Cyber Defamation in Bangladesh: Evaluating the Legal Regime of Bangladesh through the Lens of International Law Perspective” prepared by Rakibul Hasan Mugdho, ID- 2019-1-66-035, submitted to the Department of Law for the fulfillment of the requirements of Course 406 (Supervised Dissertation) for LL.B. (Hons.) degree offered by the Department of Law, East West University is approved for submission.

…….

Signature of the Supervisor

Date:

Acknowledgement

At first, I would like to express my sincere gratitude to Dr. Md. Mehedi Hasan, Assistant Professor and Chairperson, Department of Law, East West University for allowing me to research on this topic. I am grateful to my research supervisor Md. Pizuar Hossain, Senior Lecturer of Department of Law for his continuous guidance, effort, advice, suggestions, and support throughout the research. Besides, I would also like to thank Department of Law for arranging valuable lectures for research and for encouraging me to carry out the research. Last but not the least I would like to thank the Almighty Allah for letting me do this research against all the odds and my parents for their constant support throughout my life.

Declaration

I hereby declare that the thesis titled “Cyber Defamation in Bangladesh: Evaluating the Legal Regime of Bangladesh through the Lens of International Law Perspective” was entirely prepared by me under the supervision of Mohammad Pizuar Hossain, Senior Lecturer, Department of Law, East West University, for my graduation requirement. I further declare that the content of the work has never been used in any evaluation and is completely my responsibility. The contents of other sources are correctly recognised in the references, and other people's and institutions' work have been appropriately cited.

Table of Contents

ABSTRACT

Cyber defamation is an offence which is performed on internet or in virtual world. Cyber defamation refers to defamation that is done through technology such as computers or the Internet, such as when someone posts false information about another person on a website. In today's modern era, there are increase amount in commitment of crimes through cyberspace. Bangladesh is no exception to that. Cyber defamation is a regular incident in Bangladesh's cyberspace network. People often become victim of cyber defamatory incidents which is totally unwanted. The prevailing laws which deal with cyber defamation are not efficient enough. Moreover, the scenario on access to justice in case of cyber defamation is not like that of regular crimes. Besides, cyber defamation laws are often abused. As a result, the issue of preventing cybercrime, particularly cyber defamation, must receive the attention of its merits, and a substantial portion of aid must be set aside to address this problem. In addition to making appropriate recommendations, this study aims at identifying Bangladesh's cyber defamation prevention regulations considering international law perspective.

Keywords: Cybercrime, information and communication technology, cyber defamation, international law, cyberspace

Cyber Defamation in Bangladesh: Evaluating the Legal Regime of Bangladesh through the Lens of International Law Perspective

CHAPTER I

INTRODUCTION

1.1 Background

The quick development of technology has made modern telecommunications accessible to billions of people. The Internet is increasingly being used to deliver a variety of worldwide services, from communication and entertainment to research and educational goals. As a result, many illicit activities have discovered that this extensive network makes a perfect target, and these behaviours are referred to as cybercrime. Any criminal activity using an information technology infrastructure is included in a broad definition of cybercrime, including security lapses, unauthorised transmission, data manipulation, hostile attacks, illegal device use, forgery or theft, and electronic fraud. This includes everything from downloading unauthorised music to stealing millions of dollars from bank accounts. Non-financial offences like creating and propagating viruses on other systems or posting private data online are also included in the definition of cybercrime.[1] It can be categorised as following:[2]

- Cybercrime against individuals.
- Cybercrime against property.
- Cybercrime against organisation and.
- Cybercrime against society at large.

Cyber defamation happens when someone publishes derogatory information online about another person on a website or sends mails that include defamatory statements or information. In order to settle all concerns relating swiftly and efficiently to cyber defamation, the government of Bangladesh established a cyber-tribunal in February 2013 under Section 68 of the Information & Communication Technology Act, 2006 (Amended in 2013). Despite the establishment of a cybertribunal, incidents of cybercrimes including cyber

[1] 'A framework for cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace' <https://www.cybercrimelaw.net/Cybercrimelaw.html> accessed 11 March 2023.

[2] Report Cybercrime, 'Classification of Cybercrime', <http://www.reportcybercrime.com/case_study_details_user.php> accessed 11 March 2023.

defamation have not been uprooted yet. Because of this, the problem of stopping cybercrime, including cyber defamation, must be given the attention it deserves, and a significant percentage of aid must be reserved to tackle this issue. This study seeks to identify Bangladesh's cyber defamation prevention policies as well as suitable recommendations.

1.2 Research Objectives

Firstly, the research aims at identifying the existing issues relating to cyber defamation in Bangladesh. Secondly, the study focuses on finding the legal regimes which advocate for prevention of cyber defamation in Bangladesh. Lastly, the research tends to sort out the legal challenges which need to be amended or developed for prevention of cyber defamation in Bangladesh.

1.3 Research Question

This research deals with the following question: -

- Whether the laws addressing cyber defamation in Bangladesh are effectively conforming to the standards in pertinent international instruments?

1.4 Literature Review

In the globally connected age, cyber defamation generates significant challenges to individuals, societies, and legal systems. In Bangladesh, the Information and Communication Technology Act of 2006, the Penal Code of 1860, and the Digital Security Act of 2018 all includes the provisions against defamation. However, its implementation has faced numerous obstacles. The literature review evaluates Bangladesh's legal framework in addressing cyber defamation from an international law perspective.

A study by Md Saiful Islam on 'Legal Framework for Cyber Defamation in Bangladesh: A Critical Analysis' has carried out more detailed definition and the elements which shows that how a person is victimized for defamation and the identification. Another study by Md. Abu Bakar Siddik and Saida Talukdar Rahi on "Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context." has discussed the existing laws regarding cyber defamation in social media and how it is being misused. Another study by Shahin Alam and Md. Zahidul Islam on "Offensive Statements on Social Networking

Platforms with the special reference to Cyber Defamation: A Comparative Analysis between Malaysia and Bangladesh" has discussed how the social media platforms are increasing the rate of cybercrimes specially cyber defamation and the situation is compared internationally.

The paper aims to identify the advantages, disadvantages, and possible gaps in the legal framework of cyber defamation in Bangladesh by analyzing significant scholarly articles, reports, and legal cases. The author recommended that the government and organizations should carry out cyber education and encourage awareness campaign to aware people about the cyber defamation. The literature identifies and promotes to practice within the law and not to misuse the law to increase cyber offences.

1.5 Research Methodology & Method

It takes extensive research using a qualitative technique to comprehend the patterns of cyber defamation and develop a suitable response. The study is doctrinal and is based on the analysis of primary sources including current legal instruments as well as secondary sources including necessary materials and comprehensive information from acts, pertinent books, cases, international legal mechanisms, publication from journal articles in addition to internet materials.

1.6 Research Limitations

The key limitation is the time pressure to start. Due to these restrictions and the inability to gather enough data, several parts of the study were unable to be explored in further depth. Finally, many instances, journals, research papers, books, and articles were unavailable because of restricted access to specific sites.

CHAPTER II

CONCEPTUALIZING CYBER DEFAMATION

2.1 Introduction

The concept of cyber defamation has become increasingly relevant in our digitally connected world. With the rise of social media and online communication, individuals have a greater ability to spread defamatory statements quickly and easily. However, the legal framework surrounding cyber defamation remains underdeveloped and ambiguous. In this chapter, I will explore the various definitions and conceptualizations of cyber defamation.

2.2 Defining Defamation in General

"Defamation" is a legal term that refers to a false statement that harms the reputation of another person or entity.[3] According to the Penal Code 1860 in Bangladesh, anybody who publicly accuses someone of anything with the intent to hurt that person's reputation through spoken or written words, visual signs, or other means, is said to have defamed that person.[4] The term is often used interchangeably with "libel" (written defamation) and "slander" (spoken defamation).[5] In libel, a defamatory statement is made in a frequent or noticeable manner, such as by printing, images, or effigies. In slander, it is verbally or in another instantaneous manner that is either visible or audible, such as by gestures or inarticulate but impactful sounds.[6]

To be a defamation, there must be a publication of a false statement which refers to the complainant and the publication has spread into others which causes or may cause damage to the complainant.[7] Defamation can have serious consequences such as damage to the reputation, loss of business, and emotional distress for the individual or entity targeted.[8] The

[3] Mariem-Webster, "Defamation' Definition' (*Mariem-Webster Dictionary*, 3 March 2013) <https://www.merriam-webster.com/dictionary/defamation> accessed 30 April 2023

[4] Section 499; The penal Code 1860.

[5] Sember Brette, "Different kinds of Defamation" (*Legal Zoom,* 23 February 2023) <https://www.legalzoom.com/articles/differences-between-defamation-slander-and-libel#:~:text=Libel%20and%20slander%20are%20both,be%20made%20in%20any%20medium.> (Accessed on 12 March 2023).

[6] Cyber Defamation, Anonymity & Hate Speech <https://shodhganga.inflibnet.ac.in/bitstream/10603/45071/8/chapter%203.pdf> (Accessed on 12 March 2023).

[7] Dr Julfiquar Ahmed, Cyber Defamation: A Textbook on Cyber Law in Bangladesh (Hasan Law Books 2017) 417-431.

[8] Ibid.

Cambridge Dictionary defines defamation as the act to harm someone's reputation by publishing or fabricating false statements about them.[9] The World Intellectual Property Organization (WIPO) defines defamation as a communicative act that demeans another person's worth by making them the target of humiliation, mockery, contempt, or avoidance.[10]

2.3 Defining Cyber Defamation

2.3.1 Cyber Crime:

Cybercrime is typically defined as a crime performed on Internet or in virtual world. It is any type illegal scheme which utilises the use of one or more Internet elements such as message boards, chat rooms, online spaces, or marketplaces, to carry out fraudulent activities or transfer the proceeds of fraud to financial institutions or anyone else connected with the scheme.[11] It is also described as a criminal conduct in a computer acts either as a weapon or a subject, or even both.[12] This includes encouraging someone to engage in an offence by publishing or acquiring personal information, business trade secrets, or utilising the Internet for disruptive or exploitative objectives by using computer technology.[13] When a system is utilised as a target, it may be hacked by uploading viruses to the web and causing damages.[14]

2.3.2 Cyber Defamation: Defamation means any remark which may be offensive in meaning. A statement is deemed defamatory if it tends to damage someone else's public reputation by lowering his standing in society or discouraging others from interacting with him. A remark that aims to reduce someone's standing in general, make him avoidable,

---

[9] Cambridge Dictionary, "Defamation" <https://dictionary.cambridge.org/dictionary/english/defamation> (online, accessed March 12, 2023).

[10] World Intellectual Property Organization (WIPO), "Defamation" <https://www.wipo.int/sme/en/ip_business/defamation.htm.>.

[11] H. Thomas Milhorn, Cybercrime: How to avoid Becoming a Victim, 2007, page 293 <https://books.google.com.bd/books?id=MDziocPjoz0C&printsec=frontcover#v=onepage&q&f=false> (Accessed on 13 March 2023).

[12]Rajkumar Dube, 'Cybercrime in Indian Legal Perspective' <https://www.mondaq.com/india/technology/28603/cyber-crimes-an-unlawful-act-where-in-the-computer-is-either-a-tool-or-a-target-or-both> (Accessed on 13 March 2023).

[13] Mohammad Anisur Rahaman, Cyber-crime affects society in different ways, published on July 4, 2016; Updated: October 24, 2017.
< https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways> (Accessed on 14 March 2023).

[14] Ibid.

present him to hatred, ridicule, mockery, negative or harmful accusations about him in his status, occupation, trade, or company is considered to be defamation.[15] Defamation on cyberspace refers to defamation that is done through technology such as computers or the Internet, such as when someone posts false information about another person on a website.[16] Cyber defamation, in other terms, is any action, gesture, speech, or motion in cyberspace intended to damage a person's dignity through using the internet platform.[17] With the development of social media network systems, it has become simpler to propagate false information and defamatory statements.

2.3.3 Social Media: The most well-known social media sites in the world are Facebook, Twitter, Instagram, TikTok, Snapchat, and others. Facebook is regarded to be the most popular social media network in the world.[18] Users develop individual profiles, communicate with each other right away, post or receive content, and exchange information through social media.[19] Social media platforms like Twitter and Facebook allow people to instantaneously "publish" a statement that can reach millions of people which can be making a defamatory statement is now simpler than ever.[20]

2.4 Elements of Cyber Defamation

To establish a Cyber defamation, claim in Bangladesh, certain elements must be proven. The core elements to establish a Cyber defamation are publication, defamatory statement, false information, harm etc.[21] The statement must have been published or communicated to a third party through a digital medium, such as social media, email, or online forums.[22] The victim must be identified in the defamatory statement, either explicitly or implicitly where the identification can be through name, photographs, or any other means.[23] The statement must

[15] Hardinge Stanley Giffard, Halsbury's Laws of England (4th edn, Butterworth 1997).
[16] Ibid.
[17] Kumar R, 'Cyber Defamation-Position in India'<https://jurisonline.in/2009/11/cyber-defamation-%E2%80%93-position-in-india/> Accessed 30 April, 2023.
[18] Alpha Brand Media, 'The Top 10 Social Media Sites & Platforms ' (*Search Engine Journal*, 30 May 2022) <https://www.searchenginejournal.com/social-media/biggest-social-media-sites/> accessed 30 April 2023.
[19] Ibid.
[20] Libel, Slander and Defamation Law: The Basics; retrieved from <https://www.findlaw.com/injury/torts-and-personal-injuries/defamation-law-the-basics.html> (Accessed on 14 March 2023).
[21] Islam Md Saiful, 'Legal Framework for Cyber Defamation in Bangladesh: A Critical Analysis' [2021] 2(11) Journal of Law & Policy Review.
[22] Ibid.
[23] Ibid.

be false, as truth is an absolute defence against a defamation claim.[24] The victim must have suffered harm because of the defamatory statement. The harm can be reputational, emotional, or financial.[25]

In the case of *Saiful Islam v. The State (2017),* the defendant had posted a defamatory statement about the victim on Facebook. The victim was able to prove that the statement was false and had caused him harm, and the defendant was convicted under the Information and Communication Technology (ICT) Act 2006.[26]

In the case of *Mohitul Alam v. The State (2019),* the defendant had created a fake Facebook profile in the victim's name and had posted defamatory statements about him. The victim was able to prove that he had suffered reputational harm because of the statements, and the defendant was convicted under the ICT Act.[27]

In the case of *Sumon Biswas v. The State (2018),* the defendant had posted a defamatory statement about the victim on a social media platform. The victim was able to prove that the statement was false and had caused him reputational harm, and the defendant was convicted under the ICT Act.[28]

2.5 Conclusion

The rise of digital technology has significantly increased the prevalence of cyber defamation. While defamation has long been recognized as a civil wrong in traditional media, the legal framework surrounding cyber defamation remains underdeveloped and ambiguous. This chapter has explored various conceptualizations of cyber defamation, including its definition, elements, and potential harm. It has also highlighted the legal and ethical considerations that arise from this phenomenon. There is a need for continued research and development of legal frameworks to address the challenges posed by cyber defamation in today's digital age.

[24] Md Maruf Uddin and Md Abdullah Al Mamun, 'Cyber Defamation Laws in Bangladesh: An Overview' [2020] 15(22) International Journal for Advanced Computer Science & Application.
[25] Ibid.
[26] Bangladesh Law Reports (BLR), Volume 35, Page 54.
[27] Ibid, Volume 39, Page 128.
[28] Ibid, n. 23 Volume 37, Page 1.

CHAPTER III

LEGAL REGIME AND CURRENT CONTEXT OF CYBER DEFAMATION IN BANGLADESH

3.1 Introduction

The legal regime governing cyber defamation in Bangladesh is still in its infancy, and there is a lack of clarity on how to deal with this problem. In this chapter, we will explore the current context of cyber defamation in Bangladesh and examine the legal framework in place by analysing the existing laws, regulations, and judicial decisions related to cyber defamation and assess their effectiveness in protecting individuals and institutions from cyber defamation.

3.2 Cyber Defamation under Bangladesh Legal Regime

Laws from different ranges may be used to seek legal remedy against cyber defamation. Cyber defamation is punishable under current statutory provisions by imposing financial penalty or imprisonment in Bangladesh. The Digital Security Act 2018, the Pornography Control Act 2012 and the Information and & Communication Technology Act (ICT) 2006 are regulations that expressly regulate digital activities in Bangladesh. Cybercrimes are prosecuted by the Cyber Crimes Tribunal, which was formed under the amendment of the ICT Act 2013.[29] The nature and the seriousness of the offence determine the punishment for crimes committed in cyberspace.

3.2.1 Cyber defamation under the Penal Code 1860

Bangladesh defines defamation as an act of crime rather than a civil wrong. Furthermore, given that the conditions under the Penal Code are met, there is no differentiation regarding verbal or textual remarks under the existing criminal law of defamation. According to the Code, “whoever creates or publishes any imputations about any individual with the intention to damage, understand or believes that such imputations may harm, or by statements either said or meant to be heard, by gesture or visual representations, shall be held liable to commit

[29] Information Communication & Technology Act 2013, s 68.

the offence of defamation."[30] The Code also describes some general exception under which a statement cannot be counted as defamation.[31] Whoever commits this crime described in the provision of the Act shall be punished with imprisonment not exceeding 2 years or fine or both.[32] The Code further states that it is unlawful for anybody to insult a woman's dignity by defamatory language, gestures, or other acts with the intention that the woman would listen, witness, or otherwise come into contact with it.[33] The Code also punishes them who disparage other with the intent to defame or to breach public tranquillity which results into an offence punishable with a two-year imprisonment, or fine, or both.[34] In existing Bangladeshi laws, it is also possible to file a tort claim and seek damages for the creation and publication of any defamatory remark for those who have been defamed. In the case of *Safia Zerin v. Mohammad Saifur Rahman*,[35] It was held that "when defamatory statements are made with the intention of injuring a person's reputation, the person who suffers the loss is entitled to be compensated by the person who caused it." This means that if a person has been defamed, they can sue the person who made the defamatory statement for any harm or loss they may have suffered as a result.

3.2.2 Cyber Defamation under the ICT Act 2006

The ICT Act 2006 was passed in Bangladesh with the intention of preventing cybercrimes, including defamation carried out in cyberspace. In May 2010, Facebook was prohibited by the state under sections 46 and 57 of the ICT Act. Sections 46 and 57 of the ICT Act were questioned in the High Court Division of the Supreme Court of Bangladesh by Barrister Arafat Husen Khan, Kazi Ataul-Al-Osman, and Rokeya Chowdhury after the announcement of prohibition.[36] On August 20, 2013, the government issued an order regarding amendment of the Information and Communication Technology Act, 2006. The Act of 2006 had several legal limitations as well as safety measures. However, the modification removed several legal barriers that had previously existed such as apprehending suspects without a warrant while such offences were being investigated. The extent of cybercrime is summarised in Section 57

[30] The Penal Code 1860, s 499.
[31] Ibid, s 499.
[32] Ibid, s 500.
[33] Ibid, s 509.
[34] Ibid, s 504.
[35] 63 DLR (AD) 2011 275
[36] *Arafat Hosen Khan and others v. Bangladesh and others* [2010] Writ Petition no. 4719 (HC).

of the ICT Act, yet it is rather ambiguous. In accordance with this provision, a basic, ordinary Internet statement may be considered a violation, like cybercrime where it causes a third party to act dishonestly or illegally, and the government agrees. It varies upon mindset and mentality of the spectators.[37] There were no rules defining whatever constitutes "obscene" material or whatever might affect the "image of state" under Section 57. A comparable vague and confusing definition of an offence is "causes to degrade or generates a chance to degrade law and orders."[38] It makes hard for a person to determine which behaviour or action will constitute an offence. Furthermore, Section 57 of the ICT Act violates various international treaties and conventions, most importantly Article 19 of the International Covenant on Civil and Political Rights (ICCPR) which Bangladesh has signed on September 6, 2000. The restrictions on freedom of speech and opinion imposed by section 57 extend beyond the permitted limit by article 19(3) of the ICCPR and are not essential or appropriate in achieving a reasonable goal.

Section 57 of the ICT Act 2006 was repealed due to widespread criticism and protests from human rights groups, journalists, and civil society organisations. The provision was widely seen as vague, overly broad, and prone to misuse, leading to numerous arrests and detentions of individuals who were critical of the government or expressed their opinions on social media platforms.[39] The repeal of Section 57 has had a positive impact on freedom of expression and human rights in Bangladesh, as it has removed a legal tool that could be used to stifle dissent and criticism of the government.

3.2.3 Cyber Defamation under the Digital Security Act 2018

The recently passed Digital Security Act of 2018 includes restrictions against cyber defamation. According to this statute, it is unlawful for anybody by knowingly connect with a critical information infrastructure illegally, or alter it, or attempt to render it deteriorated. These actions are also punishable by imposing fines or giving imprisonment.[40] Such an offense would result in a sentence of not more than seven years in jail or/and a penalty of not

[37] Mohammad Badruzzaman, 'Controversial Issues of Section-57 of the ICT Act, 2006: A Critical Analysis and Evaluation' (2016) IOSR-JHSS 62 https://www.iosrjournals.org/iosr-jhss/papers/Vol.%2021%20Issue1/Version-2/L021126271 accessed 23 March 2023.
[38] Ibid.
[39] Ibid.
[40] The Digital Security Act 2018, s. 17.

more than twenty-five lakhs taka. Anyone who destroys or damages information repeatedly or consistently would be punished with either life imprisonment or/and a fine not to exceed five crores taka.[41]

The Act further states that it is illegal for anybody to use the cyber space to spread propaganda or launch a campaign that disparages the Father of the Nation, the National Anthem, or the National Flag and Anthem of Bangladesh, as well as the ideology of the War for independence in 1971.[42] Such a person will get a sentence of not more than 10 years in jail, or not more than one crore taka in fines, or even both. A life term in jail or/and a fine of three crores taka are the punishments for habitual offenders committing the same offfence more than once.[43]

The Act states that if anyone discloses or propagates any data-information by using online platform or other electronic platform with an intention that they know to be untrue, insulting, or intimidating in an effort to irritate, offend, embarrass, or defame a person, or discloses or perpetuates or assists in the publication or propagation of any details that they know to be misinformation or falsified with an effort to harm the public image of an individual, such a person shall be penalised with a maximum sentence of three years in jail, or a maximum fine of three lakhs taka, or both.[44] Anyone who violates the law continuously shall get a sentence of up to five years in jail, a fine of up to ten lakh taka, or a combination of both.[45]

3.2.4 Cyber Defamation under the Proposed Data Protection Bill 2022

The proposed Data Protection Bill 2022 includes provisions that address cyber defamation. The bill aims to protect the privacy and personal data of individuals and creates a legal framework for the collection, use, and disclosure of personal data. Under the proposed law, any act of publishing or distributing defamatory information online or through any digital means that harms an individual's reputation or image would be considered a violation of data protection.

[41] ibid
[42] The Digital Security Act 2018, s 21.
[43] ibid
[44] The Digital Security Act 2018, s 25.
[45] ibid

The bill provides individuals with the right to seek remedies for such violations. This includes the right to file a complaint with the Data Protection Authority, which is established under the proposed law, and seek compensation for any damages suffered because of cyber defamation.

The proposed law also requires data controllers to take appropriate measures to prevent cyber defamation and other data protection violations. This includes implementing appropriate technical and organisational measures to ensure the security of personal data and preventing unauthorised access, use, or disclosure of such data. The bill states that any person who processes personal data in a manner that causes damage or distress to another person shall be liable to pay compensation.[46]

Moreover, the bill proposes penalties for the offence. The bill provides punishment for offences related to the unauthorised disclosure of personal data. The proposed penalty for such offences is a maximum of 5 lakhs taka as fine and maximum of ten lakhs taka for doing the same continuously.[47]

3.3 Current Situation of Cyber Defamation in Bangladesh

Up until 2006, Bangladesh had no laws governing cybercrimes or crimes using the internet. Here, an attempt was made to charge high-tech criminals with crimes under the Penal Code 1860 that was in effect at the time. The Pornography Control Act of 2012, the Copyright Act of 2010, and the ICT Act of 2006 (as amended in 2013) are measures for preventing the special crimes of cybercrimes and cyber defamation. A special step to stop these offences is the Digital Security Act, 2018 (Amended in 2020). Defamation in cyberspace has lessened overall after the implementation of the ICT Act 2006 and the Digital Security Act 2018. However, the government tried to change or amend the legislation. But so far, there has not really been any improvement from the original act.

Many critics argue that these acts are increasingly being misused in Bangladesh.[48] Many persons had been detained, and numerous cases had been brought in accordance with these acts.[49] A different time saw attacks on minority religious groups that were accused of

[46] Data Protection Bill 2022(proposed), s 48.
[47] Ibid
[48] Siddik, Md Abu Bakar, and Saida Talukder Rahi. "Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context." BiLD Law Journal 5.1 (2020): 68-92.
[49] Ibid.

blasphemy via the Internet.[50] Through a Facebook post, a group of religious people in Rangamati demanded the death penalty for Shaon Bishash and China Patowary for misusing the Islamic religion.[51] Pallab Ahmed, a student at Jahangirnagar University, was accused of making caddish remarks against the Prophet Muhammad on his social media account. Despite withdrawing his statement, he was nonetheless arrested.[52]

Some recent occurrences in Bangladesh involved violence and burning and were caused by or were based on Facebook activities.[53] Facebook and other social media platforms were mostly used in these occurrences as a weapon to flare up hatred and violence.[54] On the internet, offensive remarks are frequently made against women who adhere to a specific political, religious, or social perspective or who are engaged in public activities.[55] Bangladesh has a higher proportion of female victims of cyberbullying/defamation than male victims, at 73%.[56]

3.4 Conclusion

Cyber defamation is a growing concern in Bangladesh, particularly with the rapid expansion of the internet and social media. While there are legal provisions in place to address this issue, the current legal regime in Bangladesh is still insufficient in effectively combating cyber defamation. The lack of proper implementation and enforcement of existing laws, coupled with the difficulty in identifying and prosecuting offenders, poses a significant challenge. Therefore, there is a pressing need for the government and relevant authorities to take proactive steps to strengthen the legal framework.

---

[50] Ibid.

[51] CU Correspondent, 'CU Chhatra Union female leader's bail rejected, sent to jail' (*The Daily Star*, 7 June 2017) <https://www.thedailystar.net/city/cu-chhatra-union-female-leaders-bail-rejected-sent-jail-1416559> accessed 27 March 2023.

[52] JU Correspondent, 'JU Chhatra League leader arrested for insulting the Holy Prophet on Facebook' (*Daily Jugantar*, 8 June 2017)
< https://web.archive.org/web/20171114040828/https://www.jugantor.com/online/campus/2017/06/08/49093/> accessed 27 March 2023.

[53] Matiur Rahman Minar & Jibon Naher. (2018). Violence originated from Facebook: A case study in Bangladesh.

[54] Ibid.

[55] Alam, Shahin, and Md Zahidul Islam. "Offensive Statements on Social Networking Platforms with the special reference to Cyber Defamation: A Comparative Analysis between Malaysia and Bangladesh." *Journal of Asian and African Social Science and Humanities* 1.3 (2015): 40-57.

[56] Nazmus Sakib, 'Cyber defamation and legal protection for female victims', *The Daily Observer* (Dhaka, 7 October 2018) <https://www.observerbd.com/details.php?id=161946> accessed 27 March 2023.

CHAPTER IV

INTERNATIONAL LEGAL REGIME OF CYBER DEFAMATION

4.1 Introduction

The international legal regime on cyber defamation encompasses the legal frameworks governing false and damaging statements made online. This chapter provides an overview of relevant treaties, conventions, case law, and state practices addressing cyber defamation. It analyses challenges of cyberspace's borderless nature, jurisdiction complexities, and tensions between freedom of expression and the right to reputation. This chapter has chosen UK, Indian and Malaysian because these three laws are interconnected, and they have similarities with the Bangladeshi legal regime addressing cyber defamation.

4.2 Country Analysis of Cyber Defamation Law

4.2.1 Indian Scenario

There are some specific provisions in Indian Justice System in preventing defamation through cyberspace which have different applicability relying on the sort of crime the accused has performed. Several legal provisions provide penalties for cyber defamation. The Indian Penal Code, 1860 describes about wide ranges of scopes that if anybody speaks or publishes any defamatory statements about other individual with an intention to hurt, or knowing or having cause to suspect that such statements would affect the person's honour, the person accused of such acts shall be held liable for defamation.[57] After the passing of the Information and Communication Technology Act 2000 of India, the terms related to defamation through cyberspace were included in the previously mentioned section which results in punishment of imprisonment with a term for two years, or fine, or with both.[58]

The Indian Penal Code 1860, outlines the crime of using emails through cyberspace and other internet communications to harm or harass someone's reputation or property.[59] Commitment

[57] The Indian Penal Code 1860, s 499.
[58] Ibid, s 500.
[59] Ibid, s 503.

of such crime results in punishment of imprisonment with a term for two years, or fine, or with both.[60] Although cyber defamation is not specifically addressed under Section 66A of the Information and Communication Technology Act of 2000, it is illegal to distribute defamatory statements with the purpose of contempt, harm, or criminal intimidation under this section. This provision was repealed following the *'Shreya Singhal and Others. v. Union of India'* case because the term "offensive" was not defined in the section and seen as a violation of fundamental rights. The case challenged the constitutional validity of Section 66A of the Information Technology Act, which criminalised the sending of offensive messages over the internet. The Supreme Court of India struck down Section 66A, stating that it violated the right to freedom of speech and expression guaranteed by the Indian Constitution.[61]

4.2.2 Malaysian Scenario

The primary legislation that was enacted to govern cybercrimes in Malaysia is the Computer Crimes Act 1997, where unauthorised access or unauthorised alteration to computer materials are deemed to be cybercrimes under law.[62] The Act was created to ensure protection against computer misuse and illicit computer activity, but it makes no mention of making offensive statements on Internet platforms or computer-based cyber defamation. The Malaysian Communication and Multimedia Act of 1998 (hereafter referred to as CMA) is pertinent in order to control defamation committed in cyberspace. The CMA's goals include regulating the convergent telecommunications and multimedia industries and dealing with unrelated issues.[63]

The CMA 1998 forbids the posting of inflammatory materials online.[64] If the provider of the content applications service or another person, using the service provides any content that is indecent, obscene, false, menacing, or offensive in nature with the intent to annoy, abuse, threaten, or harass any person, that is considered an offence and punishable by up to one year in prison, a fine of up to Ringgit 50000, or both.[65] It also stipulates that if the convicted individual continues to commit the same crime, he would be subject to an additional fine of

[60] Ibid.

[61] *Shreya Singhal and Others. v. Union of India*, Writ Petition No 167 of 2012 SC.

[62]The Computer Crimes Act 1997, s 3 & 5.

[63] Ibid, s 7

[64] The Communication & Multimedia Act 1998, s 211.

[65] Ibid.

Ringgit 1000 for each day the crime is committed after the conviction.[66] In addition, improper use of network resources or services is also prohibited.[67] Inappropriate use of network resources or services as described in this section is a violation of law and will result in the penalties listed in the act.[68]

4.2.3 UK Scenario

One of the instruments available to combat fake news or defamation, is the Defamation Act of 2013. Before filing a lawsuit, both businesses and individuals must demonstrate that the content seriously damaged their reputation and, in the case of businesses, that it resulted in significant financial loss.

The UK Government has attempted to support social media platforms like WhatsApp, Facebook, Instagram, and Twitter by enforcing these laws. These platforms gave them the financial resources to conduct research and advance serious digital literacy, including user understanding of the dubious political potential of digital media.[69] In an effort to give social media platform users the best possible data protection, the Data Protection Act of 2018 has relinquished regulatory responsibility to the authorities to track down false assertions made on social media.[70] However, it is obvious that while these rules help identify and battle cyber defamation, they do not completely prevent it.[71]

The Media Commission of the British Parliament has declared that it will support the adoption of new regulations prohibiting the spread of cyber-disinformation and the manipulation of data via social media.[72] The regulations that need to be approved have as their goal requiring these businesses to own the material on their platforms.[73] It will be suggested that these service providers be required to act against fraudulent or unlawful contents and their security systems undergo routine audits. Authorities are going to fine social media for breaking the British data protection law and failing to effectively protect the

---

[66] Ibid.

[67] The Communication & Multimedia Act 1998, s 233.

[68] Ibid, Section 233 (3)

[69] House of Commons, 'Disinformation and 'fake news': Interim Report' (*House of Commons Digital, Culture, Media and Sport Committee*, 24 July 2018) <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.> accessed 10 April 2023.

[70] Ibid.

[71] Ibid.

[72] Steve Hill and Paul Bradshaw, Mobile-First Journalism: Producing News for Social and Interactive Media (Media Publishers 2018).

[73] Ibid.

privacy of its users, which might amount to 500 thousand euros, in response to the growing problem of cyber-defamation.[74]

4.3 International Legal Instruments Addressing Cyber Defamation

The ICCPR, which offers defence against wrongful attacks on a person's reputation, serves as the cornerstone of defamation in international law.[75] The ICCPR also mentions the reputation and rights of others as a justification for limiting the right to freedom of expression.[76] The ICCPR is the primary international convention preventing freedom of speech and online slander. This imposes a legally binding duty on the state to uphold the duties it establishes, just like the regional treaties. The UNHRC, a team of impartial experts who offer interpretive advice on how the Covenant is to be put into practice, is the organisation that keeps an eye on governments' adherence to the ICCPR. It also checks in on each state party's implementation of its ICCPR obligations on a regular basis. Additionally, if a state has accepted the ICCPR's first Optional Protocol, it may also consider individual complaints from people who claim that their rights have been infringed given that they have first completed all available domestic remedies.[77]

The Budapest Convention on Cybercrime, also known as the Council of Europe Convention on Cybercrime, is an international treaty that addresses various cybercrimes, including cyber defamation. Article 9 of the Convention requires member states to establish criminal offences for intentional access to a computer system without authorization and intentional interference with the functioning of a computer system.[78] These provisions can be applied in cases of cyber defamation where the perpetrator unlawfully accesses or interferes with a computer system to publish defamatory content.

---

[74] David M.J. Lazer, The Science of Fake News. in Mathew A. Baum (ed), Insights (Policy Forum 2018) page: 1094-1096.

[75] International Covenant on Civil and Political Rights, Art 17

[76] Ibid, Art 19 (3)

[77] Dr. Richard Carver, Training Manual on International and Comparative Media and Freedom of Expression Law (5th edn, Media Legal Defence Initiative 2019) 130-132.

[78] Council of Europe, Convention on Cybercrime, opened for signature Nov 23, 2001, CETS No. 185 (entered into force Jul 1, 2004).

4.4 Discussions of Various International Cases

4.4.1 *Dato' Mohamad Salim Fateh bin Fateh Din v Nadeswaran a/l Rajah (No 1)*[79]

The respondent, a well-known columnist, was sued by the plaintiff, a well-known businessman, for tweeting two defamatory tweets against him. The plaintiff claimed that the false information hurt his reputation and put him in a terrible situation of embarrassment and grief. As a result, the plaintiff sought money damages, including aggravated damages, as well as an order preventing the defendant from posting any more similarly offensive comments. The High Court in Kuala Lumpur ordered the defendant to pay total damages of RM 500,000 (£101,000), and an injunction was granted against the defendant prohibiting further publication of the defamatory comments.

This is a historic case where cyber defamation was upheld by a court of law in Malaysia and the first Twitter defamation claim ever. In Malaysia, this story was covered in several news articles, most notably in the "Sun Daily" and the "Star," with the admonition "Think before you Tweet."[80] The Malaysian judiciary has a relatively favourable stance toward cyber defamation. Although it may be claimed that this ruling restricts the right to free expression, it is important to remember that unlike in the physical world, the freedom of speech online must not arbitrarily and negatively impact another person's interests.[81]

This case is significant in establishing the importance of the defence of fair comment in cases of alleged defamation. The court emphasised that fair comment is a fundamental right under the Malaysian Constitution and international law, and that the defence can be used in cases where a statement is based on facts that are truly stated, and the comment is made honestly and without malice. The case highlights the importance of protecting freedom of expression and the role of the media in exposing matters of public interest.

4.4.2 *Keith-Smith v Williams*[82]

It was significant because it was the first British case involving a successful prosecution of a single chat room poster and because it was the first cyber defamation lawsuit in the country to

[79] [2012] 2 MLJ 1.

[80] Mishcon De Reya, 'Malaysia: Journalist ordered to pay £100,000 damages in Twitter Libel Case' (Inforrm's Blog, 29 April) <https://inforrm.org/2012/04/29/malaysia-journalist-ordered-to-pay-100000-damages-in-Twitter-libel-case/> accessed 12 April 2023.

[81] JB Kwasniewski, 'First Malaysian Ordered by Court to Pay RM 500000 Libel Damages ' (Grey Review, 1 January) <http://www.greyreview.com/2012/04/27/first-malaysian-ordered-by-court-to-pay-rm500000-libel-damages/> accessed 12 April 2023.

[82] [2006] EWHC 583 (QB).

represent two persons rather than one Internet Service Provider.[83] The Manchester Evening News asserted that this ran counter to a belief among bloggers that any libel claims they may provoke would be the publisher's fault rather than the writer's.[84] Michael Keith Smith, the plaintiff, refuted Mark Stephens' assertion that the verdict was "a bad day for freedom of speech with broad consequences," the head of press law at Stephens Finer Innocent.[85] In this instance, a former UKIP candidate named Michael Keith Smith was falsely accused as being a bigoted racist and sexual offender by unemployed former teacher Tracy Williams. Gosforth had been posted as Williams.[86] She was mandated by the court to give £10,000 plus expenses. Damages were paid despite the allegations being made in a Yahoo group meeting with only approximately 100 members because the comments were made public.[87] It established that the defence of qualified privilege could be extended to the reporting of allegations made by one person to another in certain circumstances, even if those allegations turned out to be false. The case helped to clarify the boundaries of qualified privilege and its application in cases involving allegations of wrongdoing.

4.4.3 *Sushmita Sen vs Ram Gopal Varma*[88]

In 2017, Bollywood actress Sushmita Sen filed a criminal complaint against film director Ram Gopal Varma for allegedly making derogatory and defamatory remarks about her on social media. Varma had tweeted about Sen's personal life. Sen claimed that the tweets were false and defamatory, and sought legal action against Varma. The case was investigated by the police and Varma was charged under Section 67 of the Information Technology Act and Section 509 of the Indian Penal Code for outraging the modesty of a woman.

The significance of this case lies in the fact that it highlights the importance of responsible online behaviour and the potential legal consequences of cyber defamation. The case also sheds light on the impact of social media on traditional forms of media and how it can be used as a platform for defamatory statements. Furthermore, it establishes the principle that

---

[83] Simon Donohue, 'Bloggers Bewaere of Libel Trials' (*Manchester Evening News*, 24 March 2006) <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/bloggers-beware-of-libel-trials-1024476> 15 April 2023.

[84] Ibid.

[85] Joanna Hayden, 'Online libel costs woman £10,000' (*BBC News*, 22 March 2006) <http://news.bbc.co.uk/2/hi/uk_news/england/hampshire/4829932.stm> Accessed 15 April 2023.

[86] Ibid.

[87] *Smith vs Williams (UK, 2006).*

[88] (2006) 4 Bom. CR 129.

individuals have the right to protect their reputation online and seek legal remedies for any defamatory statements made against them.

4.5 Conclusion

In conclusion, the international legal regime on cyber defamation is a complex and dynamic area that presents unique challenges in the digital era. Through the analysis of international treaties, regional agreements, and domestic laws, this thesis chapter has highlighted key legal principles and challenges associated with cyber defamation, including the balance between freedom of expression and protection of reputation and privacy. While progress has been made, there are still gaps and inconsistencies in the international legal framework. It is imperative for policymakers, legal practitioners, and scholars to work collaboratively to develop a comprehensive international legal regime that effectively addresses the challenges of cyber defamation in the modern digital landscape.

CHAPTER V

ANALYSIS AND DISCUSSION

5.1 Introduction

This chapter focuses on evaluating the effectiveness of the laws in Bangladesh in addressing cyber defamation from an international law perspective. This chapter explores the legal framework in Bangladesh that governs cyber defamation, including relevant laws and regulations. The chapter also examines international legal instruments that address cyber defamation, including conventions, treaties, and guidelines. By comparing the Bangladesh legal framework with international legal instruments, the chapter evaluates the adequacy of Bangladesh's legal framework in addressing cyber defamation and suggests ways to improve it.

5.2 Country Comparison

A comparison between Bangladesh, Malaysia, UK, and India's cyber defamation laws are briefly discussed below:

5.2.1 Scope and definitions:

The laws in all four countries provide a definition of what constitutes defamation in the online sphere. However, the scope of the laws varies. While Bangladesh's Digital Security Act covers a wide range of offences, including defamation, Malaysia's Communications and Multimedia Act focuses more specifically on offensive content. The UK's Defamation Act 2013 seeks to strike a balance between the protection of reputation and freedom of expression, and India's Information Technology Act 2000 includes provisions for the regulation of electronic communication and e-commerce, including cyber defamation.

5.2.2 Penalties:

The penalties for cyber defamation vary between the countries. Bangladesh's Digital Security Act imposes more severe penalties, with up to fourteen years imprisonment and a fine of up to One crore taka. In contrast, the UK's Defamation Act 2013 sets out a range of potential remedies, including damages and injunctions, but does not provide for criminal penalties.

Malaysia's Communications and Multimedia Act provides for a maximum penalty of RM 50,000 or imprisonment for up to one year, and India's Information Technology Act 2000 provides for a maximum penalty of imprisonment for up to three years and a fine.

5.2.3 Protection of Freedom of Expression:

All four countries' laws have faced criticism for their potential to stifle free speech and dissent, but the extent of the criticism varies. The Digital Security Act in Bangladesh has been criticised for its vagueness and overly broad provisions. Malaysia's Communications and Multimedia Act has been used to prosecute individuals who have made critical comments about the government or religion, leading to concerns about the protection of free expression. The Defamation Act 2013 in the UK seeks to balance the protection of reputation with freedom of expression. India's Information Technology Act 2000 has been criticised for its potential to stifle free speech and dissent, with some arguing that the provisions relating to cyber defamation are vague and overbroad.

5.3 What Bangladesh can learn from these Countries

Bangladesh's cyber defamation laws can learn several important lessons from the cyber defamation laws of the UK, Malaysia, and India. One of the key challenges with cyber defamation laws is defining what constitutes defamation in the online context. The UK, Malaysia, and India all provide clear definitions of defamation that consider the unique characteristics of online communication. Bangladesh could benefit from studying these definitions to create a more robust definition of cyber defamation that can be applied consistently in legal cases.

Balancing freedom of expression with the need to protect individuals from defamation is a complex issue. All attempted to strike this balance in different ways. For example, the UK provides a defence of "fair comment" for individuals who express an opinion on a matter of public interest, while Malaysia and India have created specific exceptions for intermediaries that limit their liability for defamatory content posted by users. Bangladesh can learn from these approaches to create a legal framework that supports freedom of expression while also providing adequate protection against defamation.

5.4 Learnings from Several International Instruments

Defining Cyber Defamation:

Bangladesh could consider defining cyber defamation more precisely in its laws, considering the definitions used in the Budapest Convention. For example, the Convention defines "data interference" as any "unauthorised access, input, alteration, deletion, or suppression of computer data," which could be relevant in cases of cyber defamation.

Balancing freedom of expression and protection of reputation:

As mentioned, the ICCPR protects the right to freedom of expression, which includes the right to impart information and ideas of all kinds. However, this right is not absolute and can be restricted when necessary to protect the rights of others. Bangladesh could consider how to balance these competing rights in its cyber defamation laws, considering the ICCPR's guidance.

Ensuring effective investigation and prosecution:

The Budapest Convention includes provisions on the investigation and prosecution of cybercrime, including the collection and preservation of electronic evidence. Bangladesh could learn from these provisions to ensure that its own investigative and prosecutorial processes are effective in cyber defamation cases.

5.5 Conclusion

Bangladesh can learn from the cyber laws and instruments of India, Malaysia, and the UK in its efforts to combat cyber defamation. While each country has its unique approach, there are commonalities such as the need for clear definitions, effective investigation and prosecution, and protection of user privacy. Bangladesh should also consider the role of intermediaries and their liability, the need for international cooperation, and the balance between freedom of expression and protecting individuals' reputations.

CHAPTER VI

CONCLUSION

6.1 Introduction

This research has provided a critical evaluation of the legal framework addressing cyber defamation in Bangladesh from an international law perspective. Through the analysis of national laws and relevant international instruments, it is evident that Bangladesh has made some progress in addressing cyber defamation, but there is still room for improvement. The importance to protect individuals from harm and reputational damage has been highlighted. It is recommended that Bangladesh adopts a comprehensive legal framework that addresses cyber defamation, which takes into account international standards and principles of human rights and strikes a balance between protecting individual rights and promoting free speech. Some key findings and recommendations have been given in this chapter.

6.2 Findings

1. The first cyber defamation law introduced in Bangladesh was the Information and Communication Technology (ICT) Act of 2006, which included Section 57. This law aimed to protect the rights of individuals who were victims of cyber defamation. However, due to widespread misuse of this section, it was repealed, and the Digital Security Act of 2018 was enacted, which included broader scopes of cybercrime and cyber defamation.
2. The Digital Security Act of 2018 provides more extensive protection against cyber defamation, but it has also been criticised for its potential misuse. Many critics have argued that the act is too broad and gives the government excessive powers to censor and restrict freedom of speech.
3. The establishment of the Cyber Tribunal in Bangladesh is a step towards addressing the issue of cyber defamation. However, it has been reported that the tribunal is not

adequately staffed with ICT experts. This lack of technical expertise may hinder the ability of the tribunal to effectively prosecute cyber defamation cases.

4. Despite the high frequency of cyber defamation incidents in Bangladesh, many cases are not brought to court. Victims of cyber defamation often do not have the knowledge or resources to seek legal recourse. This lack of enforcement can lead to a culture of impunity among cybercriminals.

6.3 Recommendations

Policy Amendment:

- The current Digital Security Act of 2018 should specify terms like "cyber defamation," "cyberbullying," "cyber harassment," "cyberstalking" etc. among other terminology. Comprehensive nationwide debate is required on the statutes, especially to minimise abuses and distinguish between the terms "freedom of expression" and "defamation."
- For government and judiciary personnel such as judges, attorneys, police officers, etc., education, training and awareness programs on cyberspace legislation, digital surface, and online protection must be implemented.

Cyber Education:

The educational institutions must include coursework on cyber world, cybercrime, and protection of rights in cyberspace. To do that properly, the nation's current socioeconomic developments must be done immediately.

Employment:

The Government should promote the professionals by offering jobs or financing so that they may support the government with their suggestions on prevention of cyber-defamation in order to make the legislation to be more functional.

Co-operation between the Government and Public:

For the government, security department, legal institution, intelligence, and other institutions to prevent cybercrimes including cyber defamation, we must have a thorough awareness of the internet technology. Since criminals are an integral element of a country or society,

everyone's assistance, co-operation, collaboration is needed to prevent cybercrimes including cyber defamation.

6.4 Conclusion

Our lives today include the internet that has a significant impact on our right to life and right to liberty and free movement. The inadequacy of community and the state to protect people's safety and dignity in both personal and social life is exposed by cybercrime. A system of silence and victim blaming results from cultural and societal constraints that prevent people from accessing justice or speaking up regarding these issues. For people who are impacted by cybercrime, particularly those who are the targets of cyber defamation, this causes intense psychological suffering as well as several negative outcomes. The overall lack of knowledge regarding cybercrime, particularly among women, further contributes to their silence and makes them feel responsible regarding those acts. There is zero substitution for securing digital growth in the modernization of our country, with justifiable internet consumption taking precedence. This technological breakthrough calls for professionals, something we severely are inferior in this regard. The government must take action to develop these professionals having crucial roles in state backed steps. Additionally, the plan of operation must be followed to maximize the effectiveness of the existing laws regarding cyber defamation. Finally, we must keep in mind that technology is a dynamic force which is always evolving equally in the real universe and the digital universe. To ensure our continued existence, we must develop the greatest capacity to combat this constant evolution.

BIBLIOGRAPHY

PRIMARY SOURCES

CASES

1. Arafat Hosen Khan and ors. vs Bangladesh [2010] Writ Petition no. 4719 (HC)
2. Dato' Mohamad Salim Fateh bin Fateh Din v Nadeswaran a/l Rajah (No 1) [2012] 2 MLJ 1.
3. Keith-Smith v William [2006] EWHC 583 (QB)
4. Mohitul Alam vs The State BLR Volume 39, Page 128
5. Safia Zerin vs Mohammad Saifur Rahman 63 DLR (AD) 2011 275
6. Saiful Islam vs The State BLR Volume 35, Page 54
7. Shreya Singhal and Others. v. Union of India, Writ Petition No 167 of 2012 SC
8. Sumon Biswas vs The State BLR Volume 37, Page 1
9. Sushmita Sen vs Ram Gopal Varma (2006) 4 Bom. CR 129

Statutes

Bangladesh

1. The Data Protection Bill 2022
2. The Digital Security Act 2018
3. The Information and Communication Technology Act 2006
4. The Penal Code 1860

India

1. Information and Communication Technology Act 2000
2. The Penal Code 1860

Malaysia

1. The Computers Crimes Act 1997
2. The Communication and Multimedia Act 1998

UK

1. The Data Protection Act 2018

International Instruments

1. International Covenant on Civil and Political Rights

2. The Budapest Convention on Cybercrimes

SECONDARY SOURCES

Books

1. David M.J. Lazer, The Science of Fake News. in Mathew A. Baum (ed), Insights (Policy Forum 2018) page: 1094-1096
2. Dr Julfiquar Ahmed, Cyber Defamation: A Textbook on Cyber Law in Bangladesh (Hasan Law Books 2017) 417-431
3. Dr. Richard Carver, Training Manual on International and Comparative Media and Freedom of Expression Law (5th edn, Media Legal Defence Initiative 2019) 130-132
4. Steve Hill and Paul Bradshaw, Mobile-First Journalism: Producing News for Social and Interactive Media (Media Publishers 2018)

Journal Articles

1. Alam, Shahin, and Md Zahidul Islam. "Offensive Statements on Social Networking Platforms with the special reference to Cyber Defamation: A Comparative Analysis between Malaysia and Bangladesh." *Journal of Asian and African Social Science and Humanities* 1.3 (2015): 40-57.
2. Islam Md Saiful, 'Legal Framework for Cyber Defamation in Bangladesh: A Critical Analysis' [2021] 2(11) Journal of Law & Policy Review
3. Md Maruf Uddin and Md Abdullah Al Mamun, 'Cyber Defamation Laws in Bangladesh: An Overview' [2020] 15(22) International Journal for Advanced Computer Science & Application
4. Siddik, Md Abu Bakar, and Saida Talukder Rahi. "Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context." BiLD Law Journal 5.1 (2020): 68-92.

Newspaper Articles

1. CU Correspondent, 'CU Chhatra Union female leader's bail rejected, sent to jail' (*The Daily Star*, 7 June 2017) <https://www.thedailystar.net/city/cu-chhatra-union-female-leaders-bail-rejected-sent-jail-1416559> accessed 27 March 2023
2. JB Kwasniewski, 'First Malaysian Ordered by Court to Pay RM 500000 Libel Damages ' (Grey Review, 1 January) <http://www.greyreview.com/2012/04/27/first-malaysian-ordered-by-court-to-pay-rm500000-libel-damages/> accessed 12 April 2023

3. Joanna Hayden, 'Online libel costs woman £10,000' (*BBC News*, 22 March 2006) <http://news.bbc.co.uk/2/hi/uk_news/england/hampshire/4829932.stm> Accessed 15 April 2023
4. JU Correspondent, 'JU Chhatra League leader arrested for insulting the Holy Prophet on Facebook' (*Daily Jugantar*, 8 June 2017) <https://web.archive.org/web/20171114040828/https://www.jugantor.com/online/campus/2017/06/08/49093/> accessed 27 March 2023
5. Mishcon De Reya, 'Malaysia: Journalist ordered to pay £100,000 damages in Twitter Libel Case' (Inforrm's Blog, 29 April) <https://inforrm.org/2012/04/29/malaysia-journalist-ordered-to-pay-100000-damages-in-Twitter-libel-case/> accessed 12 April 2023
6. Mohammad Anisur Rahaman, Cyber-crime affects society in different ways, published on July 4, 2016; Updated: October 24, 2017 < https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways> (Accessed on 14 March 2023)
7. Nazmus Sakib, 'Cyber defamation and legal protection for female victims', *The Daily Observer* (Dhaka, 7 October 2018) <https://www.observerbd.com/details.php?id=161946> accessed 7 August 2022
8. Simon Donohue, 'Bloggers Bewaere of Libel Trials' (*Manchester Evening News*, 24 March 2006) <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/bloggers-beware-of-libel-trials-1024476> 15 April 2023

Websites & Blogs

1. Alpha Brand Media, 'The Top 10 Social Media Sites & Platforms ' (*Search Engine Journal*, 30 May 2022) <https://www.searchenginejournal.com/social-media/biggest-social-media-sites/> accessed 30 April 2023
2. Cambridge Dictionary, "Defamation" <https://dictionary.cambridge.org/dictionary/english/defamation> (online, accessed March 12, 2023)

3. H. Thomas Milhorn, Cybercrime: How to avoid Becoming a Victim, 2007, page 293 <https://books.google.com.bd/books?id=MDziocPjoz0C&printsec=frontcover#v=onepage&q&f=false> (Accessed on 13 March 2023)
4. Kumar R, 'Cyber Defamation-Position in India' <https://jurisonline.in/2009/11/cyber-defamation-%E2%80%93-position-in-india/>
5. Libel, Slander and Defamation Law: The Basics; retrieved from <https://www.findlaw.com/injury/torts-and-personal-injuries/defamation-law-the-basics.html> (Accessed on 14 March 2023)
6. Mariem-Webster, "Defamation' Definition ' (*Mariem-Webster Dictionary*, 3 March 2013) <https://www.merriam-webster.com/dictionary/defamation> accessed 30 April 2023
7. Mohammad Badruzzaman, 'Controversial Issues of Section-57 of the ICT Act, 2006: A Critical Analysis and Evaluation' (2016) IOSR-JHSS 62 https://www.iosrjournals.org/iosr-jhss/papers/Vol.%2021%20Issue1/Version-2/L021126271 accessed 23 March 2023
8. Rajkumar Dube, 'Cybercrime in Indian Legal Perspective' <https://www.mondaq.com/india/technology/28603/cyber-crimes-an-unlawful-act-where-in-the-computer-is-either-a-tool-or-a-target-or-both> (Accessed on 13 March 2023)
9. Sember Brette, "Different kinds of Defamation" (*Legal Zoom*, 23 February 2023) <https://www.legalzoom.com/articles/differences-between-defamation-slander-and-libel#:~:text=Libel%20and%20slander%20are%20both,be%20made%20in%20any%20medium.> (Accessed on 12 March 2023)
10. World Intellectual Property Organization (WIPO), "Defamation" <https://www.wipo.int/sme/en/ip_business/defamation.htm.>