



A Legal Study on Combating Cyber Slavery in Bangladesh through Prevention and Protection

Dr. Md. Raziur Rahman

Associate Professor, Department of Law, Gopalganj Science and Technology University, Bangladesh

* Corresponding Author: **Dr. Md. Raziur Rahman**

Article Info

ISSN (online): 2583-6536

Volume: 04

Issue: 03

May-June 2025

Received: 05-03-2025

Accepted: 06-04-2025

Page No: 07-11

Abstract

In Bangladesh, cyber slavery has become a major issue as a result of several residents being victims of human trafficking schemes that use them in Southeast Asian online fraud activities. Victims inside these compounds are subjected to harsh mistreatment, including as incarceration, electric shocks, and beatings, particularly if they don't achieve fraud quotas. One Bangladeshi guy who was trafficked to Cambodia, Mohammad Abdus Salam, for example, spoke of being subjected to torture and forced labour while facing death. In a similar vein, another Bangladeshi, Foysal Hossain, was sold to cybercriminals in Cambodia and tortured until he met with their demands. With many of its inhabitants falling victim to dishonest recruiting practices that result in their exploitation in scam operations overseas, cyber slavery is still a major problem in Bangladesh. The study will explore stronger enforcement of anti-trafficking legislation, increased international collaboration, and extensive victim support networks are all necessary to address this epidemic. Through this study, it is advisable to govern the procedure to prevent cyber slavery in Bangladesh and explore the effective state legal structure, establish international assistance and raise public awareness on cyber slavery.

DOI: <https://doi.org/10.54660/IJL.2025.4.3.07-11>

Keywords: Cyber Crimes, Cyber Slavery, Human Trafficking, Cyber Safety, Law and Policy

Introduction

The insufficiency of existing frameworks is shown by the lack of clear legal provisions addressing cyber slavery. The convergence of cybercrime and human trafficking is where cyber slavery works, although regulations in both areas sometimes don't work well together. Anti-trafficking laws, for example, do not adequately address the digital aspects of cyber slavery, even while they target physical abuse. Similar to this, rules against cybercrime concentrate on punishing actions taken online but seldom take into account the coercion or exploitation that led to these crimes. Cyber slavery's extraterritorial character makes things much more difficult. Victims of crimes are frequently forced to target people in another jurisdiction after being transported to another country.

While social media has made it possible for there to be previously unheard-of levels of global connectivity and has brought about numerous socioeconomic advantages ^[1] increased connectivity has also brought about new threats with real-world repercussions. There is growing evidence that social media is used to enable contemporary slavery ^[2].

¹ Lin, Y & Kant., 'Using Social Media for Citizen Participation: Contexts, Empowerment, and Inclusion', Sustainability, vol. 13, no. 12, 2021 p. 6635.

² United Nations Office on Drugs and Crime 2020, Global Report on Trafficking in Persons, United Nations, p. 15. Available at: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf. Last accessed on 9 February 2022.

Victims can target numerous people at once in different places, obtain their personal information, and take advantage of weaknesses while remaining anonymous online ^[3].

Simultaneously, the speed at which technology is developing has surpassed the pace at which regulatory frameworks are being developed. This has left a vacuum in governance and accountability, which has allowed hazards of modern slavery to thrive online.

Social media has been shown to enable forced commercial sexual exploitation (FCSE) of adults and children ^[4]. Social media users can be targeted for recruitment using chat features or misleading job ads, usually with the intention of fostering a connection ^[5]. For instance, eleven persons were detained in June 2021 for allegedly smuggling women and girls from Bangladesh to India for sexual exploitation after enticing them with the prospect of employment on TikTok ^[6]. After victims are recruited, social media can be utilized to record, publicize, and distribute FCSE material in addition to tracking victims' whereabouts and regulating their movements ^[7].

2. Objectives of the Study

The aim of the research on cyber slavery is to comprehend, stop, and fight the exploitation of people online. Using computers to recruit, control, exploit, and profit from people—often through forced labour, sexual exploitation, or other types of trafficking—is known as cyber slavery. This research will look at how traffickers use digital platforms, such as social media, job boards, messaging apps, or the dark web, to find, manipulate, and control victims. It will also look at how people become victims, including psychological strategies, socioeconomic factors, digital deception, awareness campaigns, educational initiatives, and digital literacy programs that help people identify and stay away from online exploitation.

This study will investigate how new technologies—such as deep fakes, block chain, and artificial intelligence—are either facilitating or preventing cyber slavery. Lastly, this article offers information and perspectives that support the creation of legislation, enforcement tactics, and international collaboration as well as awareness campaigns, educational efforts, and digital literacy projects that assist individuals in identifying and avoiding online exploitation.

3. Methodology of the Study

This study investigated the causes, venues, and effects of cyber slavery in Bangladesh using a qualitative research methodology. The technique was created to investigate victim experiences, perpetrator tactics, and civil society and law enforcement response mechanisms in order to obtain a comprehensive knowledge of how technology supports

contemporary slavery. Background and contextual information was gathered by conducting a thorough analysis of government publications, news stories, legal papers, NGO reports, and scholarly literature. To learn more about how traffickers function and engage with possible victims, online platforms (such as social media, recruiting websites, and dark web forums) were examined.

4. Meaning of Cyber Slavery

The term "cyber slavery" is a contemporary kind of exploitation in which people are tricked, persuaded, or compelled to labour in terrible conditions via digital tools or online settings. This type of human trafficking enslaves victims through digital control, monitoring, or manipulation. Social media sites like Facebook, TikTok, and Telegram are frequently used by traffickers to recruit people; they specifically target young people without employment by promising them well-paying positions overseas. After being tricked and sent to nations like Cambodia, Myanmar, or Laos, victims are compelled to participate in internet fraud, including cryptocurrency scams, in scam compounds. These enterprises, which are infamous for their terrible circumstances, are usually operated by crime syndicates and frequently involve Chinese people.

5. Types of slavery

Modern slavery takes many forms. The most common are:

5.1 Human trafficking: The transportation, recruitment, or harboring of individuals with the aim of using them as resources for forced labor, forced prostitution, forced marriage, or forced organ removal by the use of force, threats, or coercion.

5.2 Forced labour: Any labor or services that individuals are compelled to perform against their will, typically with the prospect of penalty.

5.3 Debt bondage/bonded labour: The most common type of slavery in the world. Individuals who are impoverished take out loans to pay off their debt, which means they lose control over both the debt and their working circumstances.

5.4 Descent-based slavery (where people are born into slavery): a very old form of slavery in which the position of the "slave" is inherited through the mother's side of the family and individuals are treated like property.

5.5 Child slavery: when a child is used as a means of obtaining personal benefit. Child marriage, child trafficking, child soldiers, and child domestic servitude are a few examples of this.

5.6 Forced and early marriage: when an individual is forced into marriage and is unable to divorce. The majority of child marriages qualify as servitude.

5.7 Domestic servitude: When properly controlled, domestic work and domestic servitude can be significant sources of income for numerous individuals and are not always

³ Ibid, p.15 & 19

⁴ Bangladesh trafficking gang lured girls using TikTok: Police', Al Jazeera, 9 June. Available at: <https://www.aljazeera.com/news/2021/6/9/bangladesh-trafficking-gang-lured-girls-using-tiktok-police>, last accessed on 11 July 2022.

⁵ United Nations Office on Drugs and Crime 2020, Global Report on Trafficking in Persons 2020, pp. 119-128. Available at: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf, last accessed on 11 July 2022.

⁶ Janjua, H 2022, 'Trapped via TikTok: Bangladeshi Girls Trafficked To India Are Facing Brutal Violence', Pulitzer Center, 2 June. Available at: <https://pulitzercenter.org/stories/trapped-tiktok-bangladeshi-girls-trafficked-india-are-facing-brutal-violence>, last accessed on 19 July 2022.

⁷ United Nations Office on Drugs and Crime 2020, Global Report on Trafficking in Persons 2020, pp. 119-128. Available from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf, last accessed on 11 July 2022.

synonymous with slavery. But because they might be out of sight and without legal protection when working in someone else's house, they might be especially open to mistreatment, exploitation, and enslavement.

6. The Response and Role of Bangladesh

Many people that are trafficked originate in Bangladesh. With an estimated 1.2 million individuals living in situations of modern slavery, including as forced labour and human trafficking, the country is extremely vulnerable to this kind of slavery. The government's reaction, however, has come under fire for being ineffective and having flaws in identifying and assisting survivors.

7. Laws related to slavery in Bangladesh

The contemporary phrase "cyber slavery" often refers to the exploitation of people using digital methods (such as online platforms or communication technologies, frequently through forced labour, sexual exploitation, or human trafficking. This can involve circumstances in which victims are forced to labour under duress, debt bondage, or threats, and their exploitation is enabled or sustained by technology. Although the phrase "cyber slavery" may not be used specifically in Bangladeshi legislation, there are a number of legal frameworks that are either directly or indirectly relevant to preventing cyber slavery.

7.1 Bangladesh Constitution ^[8]

According to Bangladesh's Constitution and current legislation, slavery is strictly prohibited. The Bangladeshi Constitution's Article 34 makes it very clear that, forced labour is prohibited. The use of force in any form is forbidden, and violators will face legal repercussions. The term "forced labour" here refers to any work or labour that is performed against the will of the individual. These consist of forced labour, slavery, human trafficking, and so on.

7.2 The Prevention and Suppression of Human Trafficking Act, 2012 ^[9]

In order to prevent and suppress human trafficking, guarantee the protection of victims' rights, and encourage safe migration, Bangladesh passed the Prevention and Suppression of Human Trafficking Act, 2012. It defines human trafficking, establishes Anti-Human Trafficking Tribunals, and specifies the punishments for a number of human trafficking-related offences. Additionally, the Act covers the establishment of safe homes for victims and offers them financial support. All forms of human trafficking, including forced labour, sexual assault, and the trafficking of organs, have been found to be illegal under the Act and punished by law. This legislation forbids and punishes trafficking in persons for the purposes of slavery, forced labour, and sexual abuse. It is crucial to remember that if the legislation is applied to validate the hiring procedure through a digital platform, cyber slavery can be prevented.

7.3 Information and Communication Technology (ICT) Act, 2006 (amended in 2013) ^[10]

According to this Act, using social media to coerce someone into doing something against their will—such as hacking, cyber-stocking, cyberbullying, etc.—will be illegal and penalised. Appropriate enforcement of this Act can also help avoid cyber slavery.

7.4 Cyber Security Act (CSA), 2023 ^[11]

(The Act has made digital and cyber crime punishable with defamation, blackmail, identity fraud and surveillance. Even though this rule has been criticised for being exploited in a number of ways, it may be utilised to combat issues like cyberslavery and blackmail.)

7.5 Child Labor (Banning and Control) Act, 2006 ^[12]

According to this act child labour under duress is illegal and is regarded as slavery as well.

7.6 Children Act, 2013 ^[13]

This law offers further protections and harsher punishments for minors who are the victims of cyber slavery. This regulation protects children from being forced into slavery, forced labour, or forced labour online.

7.7 Penal Code, 1860 ^[14]

Provisions dealing with criminal intimidation, wrongful confinement, extortion, etc., can be invoked depending on the case. Sections 370 and 371 state that purchasing or selling someone as a slave is illegal.

8. Causes of Cyber Slavery in Bangladesh

Cyber slavery, whether in Bangladesh or elsewhere, is a contemporary kind of exploitation in which people are controlled, exploited, and made wealthy by means of force, deceit, or coercion using digital technology. Cyber slavery may take many different forms in Bangladesh, where socioeconomic weaknesses coexist with rising digitisation. This is how it may appear:

8.1 Online Human Trafficking & Digital Grooming

Traffickers entice victims—particularly young women and children—with false promises of employment, marriage, or modelling chances via social media, messaging applications, and dating apps. Once confidence has been established, victims could be forced to meet in person or share private images, which might result in physical trafficking or sextortion.

8.2 Forced Online Labor (Click Farms, Fraud Rings)

People may be duped into taking "remote jobs" like data input, digital marketing, or cryptocurrency trading, only to end themselves in abusive situations. Employees could be kept in cramped quarters, made to run phoney social media profiles, defraud people online, or run phishing scams while being watched all the time.

⁸ The Constitution of the People's Republic of Bangladesh 1972 P.O. No 76 of 1972.

⁹ Act no 3 of 2012.

¹⁰ Act no 39 of 2006.

¹¹ Act no 39 of 2023.

¹² In 2006, Bangladesh passed the Labour Act, which included a section against child employment. Under this new regulation, children under the age of 14 are not allowed to work, and those under the age of 18 are not allowed to engage in dangerous kinds of child labour.

¹³ Act no 24 of 2013.

¹⁴ Act no XLV of 1860.

8.3. Sextortion and Cyber Blackmail

Criminals use compromised accounts or fictitious relationships to fool people into sharing sexual information. Following that, victims are coerced into making payments or engaging in further demeaning behaviours, which are frequently captured on camera and sold or broadcast online.

8.4 Deepfake Abuse & Revenge Porn

Fake images and films produced by AI can be used to damage reputations or engage in blackmail. Such abuse can result in forced marriages, social exclusion, or suicide in a conservative community, all of which serve to further control the victim.

8.5 Surveillance & Digital Control by Employers

GPS tracking or workplace surveillance applications may expose employees to extensive monitoring, frequently after hours. Many Bangladeshi domestic workers, particularly those in the Middle East, are subject to digital limitations that are tantamount to modern-day slavery, such as forced biometric surveillance, phone confiscation, and internet activity monitoring.

8.6 Tech-Facilitated Debt Bondage

People are drawn into debt cycles via exploitative micro lending services that have concealed conditions. Some are compelled to engage in sex work or cybercrime networks in order to pay off growing interest, which is becoming a problem among garment workers and in urban slums.

8.7 Recruitment through Fake Job Portals

False job postings either gather personal information or trick people into signing abusive contracts. Due to legal threats or seized identification, victims may be transported overseas or utilised in local cybercrime networks, with no means of escape.

9. Challenges of Cyber Slavery

Challenges in detection- Because of its anonymity, cyber slavers can operate in the digital shadows and conceal themselves behind virtual private networks (VPNs), encrypted communication channels, and pseudonyms.

9.1 Jurisdictional challenges: Since the internet crosses national boundaries, it makes legal jurisdiction more difficult. It is possible for criminals to operate from one nation while preying on people in another.

9.2 Pseudonymity: Since they frequently adopt false identities, it can be difficult to identify and track down the perpetrators.

9.3 Ephemeral evidence: Digital evidence can disappear fast because of encryption, data loss, or abrupt changes to online platforms.

9.4 Resource constraints: Staffing numbers and technology limitations affect law enforcement organisations.

10. Recommendations for Preventing Cyber Slavery

10.1 Public Awareness and Digital Education

The first line of defence is raising public awareness of cyber threats.¹⁵ Campaigns to raise awareness in the community through social media, radio, and television can assist individuals in identifying warning signs of internet

trafficking and fraud. Programs for digital literacy in community centres, schools, and universities can enable youth to defend themselves.

10.2 Strengthening Legal and Policy Frameworks

In order to address the issues of internet exploitation, the legal system must change. Revise anti-trafficking legislation to include internet recruiting fraud and digital coercion. Law enforcement should set up dedicated cybercrime units to keep an eye on, look into, and prosecute perpetrators^[16]. Make sure the immigration, trafficking, and cybercrime departments work together.

10.3 Safe and Transparent Online Platforms

Job sites and tech businesses need to be accountable for the material posted on their platforms. Collaborate with tech companies to keep an eye on and eliminate questionable job postings or content that may be predatory. Platforms should be encouraged to validate recruiters and employers. Encourage the usage of reputable employment platforms that have been established or supported by the government.

10.4 Regulating Overseas Job Recruitment

A large number of victims are trafficked while posing as foreign workers. Tighten regulation of online and offline hiring firms. Give migrant workers pre-departure training that covers emergency contacts and cyber safety. Establish official, government-backed websites that provide secure information on international migration and employment prospects.

10.5 Victim Support and Rehabilitation

Strong support networks are essential in the event that prevention fails. Provide victims of cyber slavery with reintegration services, psychological support, and legal assistance. Encourage civil society organisations and NGOs that combat human trafficking and defend the internet. Make sure victims may come forward fearlessly and anonymously to report abuse.

10.6 Collective Responsibility

The government cannot win the battle against cyber slavery on its own. It calls for a unified front from citizens, law enforcement, media, tech companies, educators, and civil society. Bangladesh has to take immediate action to prevent its citizens, particularly the young, from becoming victims of online trafficking.

We can ensure that the internet continues to be a tool for empowerment rather than exploitation by encouraging digital literacy, safe migration, strong regulations, and strong community networks.

11. Conclusion

Strict regulations and their application are urgently needed in order to raise awareness among Bangladeshis of the dangers of cyber slavery, safeguard them, and enhance the law enforcement agency's technological proficiency. Verifying psychiatric support, legal counsel, and rehabilitation for individuals confined to this slave system is crucial. Finally, Bangladesh's exploitation of cyber slavery is a complex problem linked to both economic vulnerability and legal

¹⁵ Rahman Raziur 'Textbook on Media and Cyber Law' Beacon Publications, Dhaka, 1st edn, 2022. P.136

¹⁶ Raziur Rahman, Prevention of Cyber Crimes in Bangladesh, Society and Change (Journal of Social Science), Voi. XI, No.4, October-December 2017, P.17

loopholes. Strong control, education, awareness-raising, and victim support networks must all be included in a comprehensive strategy to solve these issues.

12. References

1. The Guardian. Beatings, torture, and electric shocks: freed scam compound workers allege horrific abuse [Internet]. 2025 Feb 25. Available from: <https://www.theguardian.com/world/2025/feb/25/beatings-torture-and-electric-shocks-freed-scam-compound-workers-allege-horrific-abuse>. Last accessed on 2025 Mar 10.
2. Lin Y, Kant. Using social media for citizen participation: contexts, empowerment, and inclusion. *Sustainability*. 2021;13(12):6635.
3. United Nations Office on Drugs and Crime. Global report on trafficking in persons 2020. United Nations; 2020. p. 15. Available from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf. Last accessed on 2022 Feb 9.
4. United Nations Office on Drugs and Crime. Global report on trafficking in persons 2020. United Nations; 2020. pp. 15, 19.
5. Bangladesh trafficking gang lured girls using TikTok: police. Al Jazeera [Internet]. 2021 Jun 9. Available from: <https://www.aljazeera.com/news/2021/6/9/bangladesh-trafficking-gang-lured-girls-using-tiktok-police>. Last accessed on 2022 Jul 11.
6. United Nations Office on Drugs and Crime. Global report on trafficking in persons 2020. United Nations; 2020. pp. 119-128. Available from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf. Last accessed on 2022 Jul 11.
7. Janjua H. Trapped via TikTok: Bangladeshi girls trafficked to India are facing brutal violence. Pulitzer Center [Internet]. 2022 Jun 2. Available from: <https://pulitzercenter.org/stories/trapped-tiktok-bangladeshi-girls-trafficked-india-are-facing-brutal-violence>. Last accessed on 2022 Jul 19.
8. United Nations Office on Drugs and Crime. Global report on trafficking in persons 2020. United Nations; 2020. pp. 119-128. Available from: https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf. Last accessed on 2022 Jul 11.
9. The Constitution of the People's Republic of Bangladesh 1972. P.O. No. 76 of 1972.
10. Act No. 3 of 2012.
11. Act No. 39 of 2006.
12. Act No. 39 of 2023.
13. Bangladesh Labour Act 2006.
14. Act No. 24 of 2013.
15. Act No. XLV of 1860.
16. Rahman R. Textbook on media and cyber law. Dhaka: Beacon Publications; 2022. p. 136.
17. Rahman R. Prevention of cyber crimes in Bangladesh. *Society and Change (Journal of Social Science)*. 2017;XI(4):17.