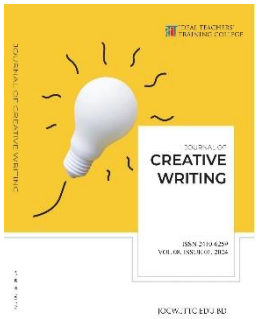

JOURNAL OF CREATIVE WRITING
VOLUME 8 ISSUE 1
2024, Pp 81-93
ISSN 2410-6259

HTTPS://DOI.ORG/10.70771/JOCW.V8I1.109

Balancing Cybersecurity And Individual Rights: A Critical Analysis Of Bangladesh's Cyber Security Act 2023

SHAMSAD BINTE EHSAN[1]
MD. NAJMUS SAQUIB[2]

ABSTRACT
Cybersecurity law is designed to safeguard national security and public safety. But it arguably raises a question: whose security is being emphasized? Although this act seeks to mitigate cyber risks and protect web infrastructure, in some instances, they also give governments an opportunity to control digital environments at the cost of individual liberties. This happens due to broad provisions and ambiguous phrasing in such legislation. In the name of monitoring individuals without sufficient accountability this act diverts attention from public safety to governmental authority. Therefore, good cybersecurity laws must be balanced, safeguarding both state interests and individual rights. This paper intends to carefully analyze the Cyber Security Act 2023 (CSA 2023) of Bangladesh. It emphasizes the effects of CSA on freedom of speech, privacy, and public confidence. This article also compares various worldwide cybersecurity frameworks to evaluate how Bangladesh's cybersecurity laws may inadvertently impede individual rights. Findings suggest that although the CSA 2023 implements strategies to improve cyber safeguards. This study indicates the need for amendments to harmonize Bangladesh's cybersecurity legislation with international norms.

KEYWORDS
Cyber Security Act 2023, Freedom of Expression, Privacy Rights, Public Trust, Human Rights

[1] Graduate Researcher, Department of Computer Science and Engineering, University of Dhaka, Email: shukti0901@gmail.com, https://orcid.org/0009-0005-1377-195X
[2] Graduate Researcher, Department of Civil Engineering, BUET, https://orcid.org/0009-0000-2108-6737

INTRODUCTION

Digital connection has become a necessary component of daily life. Particularly the Cyber Security Act 2023 (CSA 2023), Bangladesh's most current cybersecurity regulations have been passed to guard against cyberattacks for its citizens. However, fears have been expressed that apart from ensuring cyber security, individual rights, particularly the right to freedom of expression and privacy, may be hampered. Although the Cyber Security Act 2023 is the successor to the Digital Security Act 2018, it has introduced some changes that could have a major impact on citizens' rights (Budiarto et al., 2024; Aslan et al., 2023).

Why is the Cyber Security Act 2023 passed as a revised form of the Digital Security Act 2018 still facing major public indignation in Bangladesh? Why do cyber security laws in other nations not have similar public reactions? Experts fear the measure will damage people's rights of expression, privacy, and other fundamental freedoms. The Cyber Security Act 2023 was meant to solve the problems in the Digital Security Act by clarifying the reasons for its adoption. Many activists believe it has failed to allay public worries about freedom of speech, privacy and misuse of authority. Analyzing specific provisions of international cybersecurity laws will enhance public confidence. The vague definitions of the Cyber Security Act in Bangladesh are creating potential for its misuse and creating fear among the public remains understudied. The role of public trust in cybersecurity legislation and analyze how provisions of the law can undermine public trust in government and create barriers to protecting individual rights is still less understood well.

THE CURRENT PAPER

In the light of e-rights, the study will assess how far the Cyber Security Act 2023 is consistent with Bangladesh's commitments to international human rights law and how reforming certain sections of the Act can protect citizens' rights. It will analyze the controversial sections of the Act and show how the Act affects the rights and freedoms of the people. This study aims to understand the gap in public confidence in the human rights implications of this law-making process in Bangladesh, in comparison with international standards, and to identify the need for legal and procedural reforms to protect civil liberties.

BACKGROUND OF THE STUDY

We are almost global citizens now as the internet connects us everyone. Cyber threats are worldwide today rather than merely a national security issue. Cybercriminals are always seeking means of financial benefit from networks, data, systems, and activities. For many reasons, the hackers are launching their assault (Mishra et al., 2022). B. Williams claims that thieves usually pursue numerous kinds of cyberattacks. First among them are individuals who just desire money by means of illicit activity. Second kind consists of those that want intellectual property or crucial knowledge to provide them an advantage over others. Third is the risk presented from inside either from an insider de facto or inadequate security practices. Exercise of many human rights now depends on the internet and other digital technologies; so, cybersecurity is crucial to safeguard these rights from online dangers (Aslan et al., 2023; Lavorgna, 2000). Our nation has enacted the Cybersecurity Act 2023 to protect the cyberspace against any cyberattacks. But sometimes, certain parts of the statute seriously restrict individual right or freedom expression.

Human rights and cyber security have in common their need for protection. Many human rights can today only be enjoyed with the use of the internet and other digital technologies; hence cybersecurity is necessary to protect these rights from risks that may develop online (Nyst, 2016; Singh, 2023). Governments, companies, and people have to all be aware of this link and endeavor to protect cyber security in addition to human rights. As they have become more ubiquitous in our everyday life, the internet and other digital technologies have become absolutely essential for the practice of many fundamental rights.

Individuals, companies, and governments all depend on knowing this link and working to defend both cyber security and human rights. Exercising numerous human rights now depends on the internet and other digital technologies, which have become ever more common in our everyday life.

Generally speaking, people nowadays have greater access to contemporary technology innovations. The increasing user base in the digital domain corresponds with the escalating cyber danger there. Implementing some kind of legal framework or procedure is the only way to minimize these risks and protect persons, organizations, and state interests (Pajuste et al., 2022). Understanding the need for this type of a protective action, Bangladesh approved the Information Communication and Technology Act (ICT Act) in 2006. Still, this Act was not thorough and omitted certain paths of use for abuse. Passed in 2018, the Digital Security Act (DSA) aims to complement this Act and fix its discrepancies.

DSA was attacked, meantime, by some for not stopping the abuse of the ICT Act. Bangladesh adopted a complete Digital Security Law in September 2018 when the Ministry of Law, Justice, and Parliamentary Affairs there unveiled the Act of 2018. This legislative clause was passed to stop the spread of racism, sectarianism, extremism, and terrorist propaganda as well as manifestations of hate aimed at religious or ethnic minorities across print, internet, and other electronic media. The statute encompassed anything the government deemed inappropriate or obscene, and offenders risked fines or maybe lengthier jail terms. Fascinatingly, the Act let law enforcement authorities hold someone without a legal warrant. Originally passed in 2006, Section 57 of the Information and Communication Technology Act gave direction and ideas for the development of this rule. Many individuals labeled DSA as an instrument used to restrict Bangladeshi people's freedom of expression Every person's right to self-development with knowledge and wisdom for self-fulfillment consists fundamentally on their freedom of speech. Under this Act, the law enforcement authorities of Bangladesh have no arbitrary authority to arrest and imprison any person only based on suspicion (Azad, 2021; Government of the People's Republic of Bangladesh, 2019; Parliament, 2006).

The UN Human Rights Chief, Volker Türk, advised Bangladesh to stop immediately implementing the Digital Security Act on March 31, 2023. Expressing worry, Türk pointed out that the Act is being used all throughout the country to capture, threaten, and harass reporters and human rights advocates, thereby suppressing online opposition voices. During the 52nd session of the UN Human Rights Council, Volker Türk pleaded for the changes to the Digital Security Act on March 7, 2023. He underlined how urgently reforms are needed as people who exercise their right to freedom of speech and belief still suffer criminal penalties (Bangladesh: Türk Urges Immediate Suspension of Digital Security Safety Act as Media Crackdown Continues, 2023).

Minister of Law, Justice, and Parliamentary Affairs Anisul Haque reassured these concerns by underlining the country's current digital government under crisis. He underlined the need of safeguarding national interests as well as those of those who are prone to cyberattacks and other kinds of violence. Haque said, whilst appreciating the necessity for a digital security legislation, the law is not meant to be repealed. He did, however, acknowledge that legislative changes are still in works on which the need of a thorough study is emphasized (Governt Alerts to Stop Misuse of Digital Security Act: Anisul Huq, 2023).

THEORETICAL FRAMEWORK

Human rights and cybersecurity are interconnected and must both be protected. The philosophy of human rights emphasizes the need of reconciling the preservation of individual liberty with the provision of technological security. The Cybersecurity Act 2023 necessitates a balance between punitive and preventive measures and individual rights, such as freedom of expression and the right to privacy (Singh, 2023; Nyst, 2016). Freedom of expression and

the right to privacy are two basic liberties absolutely essential for balancing cybersecurity regulations with human rights. Human rights theory considers the government responsible for preserving the fundamental freedoms of its people. Bangladesh is a democratic country signing many international human rights treaties. The International Covenant on Civil and Political Rights (ICCPR) and the United Nations Universal Declaration of Human Rights (UDHR) both respect as fundamental human rights freedom of expression and the right to privacy (Nyst, 2016). While assuring cyber security, these rights may be compromised; so, the human rights approach aims to create legislation guaranteeing security while safeguarding civil liberties. One of the main liberties of people living in a democratic state is their freedom of expression as it guarantees their liberty of opinion. One should consider how the Cyber Security Act 2023 can affect expression of freedom. International human rights law holds that this right may be restricted if it is absolutely essential under certain circumstances, such as those pertaining to national security or defense of other people. Still, a cohesive legislative framework is required to guarantee that this restriction is not implemented inconsistently (Singh, 2023).

More importantly yet under international human rights conventions are our right to privacy. According to the UN General Assembly decision, nations have an obligation to protect the privacy of their citizens (UN General Assembly 2013). Under numerous conditions, the Cyber Security Act 2023 permits one to violate their right to privacy under different degrees in order of security. Clause ensuring accountability and transparency in overseeing activities and protection of personal rights should be included in cybersecurity regulations.

This article tries to suggest certain legislative changes depending on the present Cyber Security Act clauses and provisions, thereby safeguarding civil liberties. The vague and opaque language and crime definitions of the legislation might result in probable abuse (TIB, 2023.). Including the necessary changes in the Cyber Security Act 2023 would help Bangladesh to better conform with international human rights standards, therefore safeguarding the freedom and security of its people.

Cybersecurity Law: A Global Perspective

Cybersecurity laws across different countries take various approaches to protect citizens' rights. These laws are primarily enacted to safeguard public interest, ensure judicial oversight, and enhance security.

United States: Cybersecurity Information Sharing Act (CISA), 2015

A key aspect of this act is its focus on protecting information privacy and ensuring judicial oversight. The CISA promotes the exchange of cybersecurity threat information, particularly between public and private sectors. CISA not only emphasizes data protection but also includes provisions for necessary security during information exchange (Cybersecurity Information Sharing Act of 2015, 2015). Through this act, the U.S. has established an organized approach to preventing cyber threats. Overall, it has some elements that could play a significant role in developing Bangladesh's cybersecurity laws.

European Union: General Data Protection Regulation (GDPR), 2018

The European Union's GDPR safeguards the privacy of individuals and organizations. This law emphasizes transparency in data collection and processing and also has set an international standard for privacy rights (Baudot & Robson, 2017). Through GDPR, the EU has implemented strict controls on data usage alongside security measures. The characteristics of GDPR may be considered an effective model for both cybersecurity and personal rights protection of our country.

Australia: Cybersecurity Strategy 2020

Australia's Cybersecurity Strategy 2020 introduced a comprehensive framework for cybersecurity. It protects digital infrastructure and secures national interests. It involves collaboration between the government and private sector. So, it becomes an effective cybersecurity system and build public trust. (Australia's Cyber Security Strategy 2020, 2020).

India: Information Technology Act, 2000

India's Information Technology Act plays a significant role in addressing the security of electronic transactions, prevention of cybercrime, and protection of personal data. This act provides a structured framework for reducing cyber offenses, and protecting users' rights in India (Indian Parliament, 2000).

Singapore: Cybersecurity Act, 2018

Singapore's Cybersecurity Act 2018 protects essential information system. This act includes provisions for licensing and emergency response. Through this legislation, Singapore has upheld international standards for data protection. Thus, it is also a key model for cybersecurity (Cybersecurity Act 2018, 2018).

Comparative Analysis in the Context of Bangladesh

A review of these laws shows that various countries have aimed to balance public interest, privacy, and security in their cybersecurity legislation. In Bangladesh, however, the Cyber Security Act 2023 has raised concerns regarding vague provisions and potential misuse. These issues, such as unclear definitions and broad powers, present challenges in building public confidence in the law (TIB, 2023).

Table 1: Overview of Cybersecurity Acts and Regulations in Various Countries

Country	Cyber Security Act/Regulation	Key Features
United States	Cybersecurity Information Sharing Act (CISA)	This Act shares cybersecurity threat information between government and private sector; protects shared data from disclosure (*Cybersecurity Information Sharing Act of 2015*, 2015).
United Kingdom	Cyber Security Strategy (2022)	This Act Focuses on resilience, incident response, and improving cyber skills; includes measures for critical infrastructure protection (HM Government, 2022).
European Union	General Data Protection Regulation (GDPR)	GDPR Regulates data protection and privacy; includes provisions for data breach notifications and penalties for non-compliance (Baudot & Robson, 2017).
Australia	Cyber Security Strategy 2020	This Act Aims to strengthen Australia's cybersecurity posture; emphasizes collaboration with industry and international partners ("Australia's Cyber Security Strategy 2020," 2020).
India	Information Technology Act (2000)	The Information Technology Act Provides a legal framework for electronic governance, cybercrime, and cybersecurity. It also includes

Country	Cyber Security Act/Regulation	Key Features
		provisions for data protection (Indian Parliament, 2000).
Singapore	Cybersecurity Act (2018)	Cybersecurity Act Establishes a framework for the protection of critical information infrastructure and incident response; includes licensing for cybersecurity service providers (Cybersecurity Act 2018, 2018).
Japan	Cybersecurity Strategy	Cybersecurity Strategy Focuses on improving cybersecurity for government, private sectors, and individuals; emphasizes international cooperation and capacity building ("Gov. Japan," 2010).
South Africa	Cybercrimes Act (2020)	This Act Addresses cybercrime and cybersecurity; includes provisions for investigation and prosecution of cybercrimes (Government Gazette, 2021).
Russia	Federal Law on Information, Information Technologies and Protection of Information (2016)	This Law Regulates information security; emphasizes state control over information resources and cybersecurity measures for critical infrastructure (Federation, 2014).
Brazil	General Data Protection Law (LGPD)	This law Regulates data protection and privacy; requires organizations to implement security measures for personal data (*Brazilian Data Protection Law (LGPD)*, 2020).
France	Cyber Security Strategy (2016)	Cyber Security Strategy Focuses on protecting critical infrastructure and enhancing resilience against cyber threats; emphasizes cooperation with industry (Darwish & Romaniuk, 2021).
Italy	The Italian Cybersecurity Action Plan	This Plan Provides guidelines for cybersecurity governance; focuses on protecting national critical infrastructure (*THE ITALIAN CYBERSECURITY*, 2017).
Malaysia	Cybersecurity Malaysia Act (2020)	Cybersecurity Malaysia Act Establishes a framework for cybersecurity services and incident response; focuses on public and private sector collaboration (MCSS, 2020).

FREEDOM OF EXPRESSION AND PRIVACY RIGHTS: A HUMAN RIGHTS-BASED ANALYSIS

International Standards and the Role of Human Rights in Protecting Freedoms

Freedom of expression and the right to privacy are considered foundational in international human rights law. International documents such as the UDHR and ICCPR support this right. Freedom of expression includes the right to seek, receive, and impart information without interference, while privacy ensures individuals' control over their personal information (United Nations, 1948; United Nations, 1966). Scholars such as De Hert and Gutwirth (2021) argue that these rights are essential to democratic governance, as they allow for open discourse, personal autonomy, and protect against authoritarian surveillance. This foundation of human rights is critical for evaluating modern cybersecurity laws, particularly in how they balance state security concerns with civil liberties.

Freedom of Expression in the Digital Era

As digital platforms become central to public communication, cybersecurity laws have increasingly intersected with the right to freedom of expression. Scholars like MacKinnon (2022) suggest that the rise of digital surveillance tools has placed significant restrictions on free expression. Some countries passed broad and vague cyber legislation to abuse digital surveillance tools. This risk is very high in states with limited judicial oversight. It becomes worst where laws intended to curb misinformation, to suppress dissent and political opposition (MacKinnon, 2022; Singh, 2023). For example, Singh's (2023) study highlights that in many countries, such laws disproportionately affect journalists and activists, who may face penalties for critical reporting under the guise of cybersecurity concerns.

Additionally, Article 19 of the ICCPR stipulates that restrictions on freedom of expression must meet criteria of legality, necessity, and proportionality (UN Human Rights Committee, 1983). However, research by La Rue (2020) suggests that cyber laws often lack these safeguards, thereby creating a alarming effect on free speech. As in todays world, citizens rely heavily on digital platforms for expression so the citizens need clear definitions of cyber security.

Privacy Rights and the Intrusiveness of Cybersecurity Measures

Tension between cybersecurity measures and privacy protection has been noted worldwide. Generally, cyber laws empower authorities to monitor online activity in ways that may infringe upon privacy rights. The right to privacy, as outlined in Article 17 of the ICCPR, protects individuals from arbitrary or unlawful interference with their privacy, family, home, or correspondence. However, privacy is often compromised by cybersecurity laws that allow extensive data collection and surveillance (Nyst, 2016). Studies by Taylor and Floridi (2021) show that excessive data collection can erode individuals' sense of personal autonomy and create distrust toward government institutions.

Moreover, Binns and Veale (2020) argue that the digital transformation and the rapid development of surveillance technologies have made it challenging to protect privacy rights. They note that cybersecurity measures often include the storage of large amounts of data, which, if not managed securely, can lead to significant breaches of privacy. This concern is further supported by studies from Bedi (2019), which found that confidence decreases significantly when individuals perceive that their data could be accessed or misused anytime.

The Impact of Ambiguity in Cybersecurity Laws

Ambiguity in cybersecurity laws can lead to abuse because it affects freedom of expression and privacy. Research by Akdeniz and Gillespie (2019) suggests that vague language in cyber laws can be misinterpreted. Authorities justify wide-ranging surveillance measures with this misinterpretation. Similarly, Bigo et al. (2020) argue that this ambiguity not only undermines

legal clarity but also erodes public confidence in cybersecurity laws. If someone exercises their right to express opinions contrary to the state's stance, they are caught or arrested. Ambiguous terms, such as "national security threat" or "public order disturbance," are frequently cited in laws worldwide to justify actions against individuals.

The European Court of Human Rights (ECHR) has also noted the importance of legal clarity in cybersecurity legislation. In cases such as *Roman Zakharov v. Russia*, the ECHR held that surveillance measures must be adequately defined and subject to judicial oversight to prevent arbitrary interference (ECHR, 2015). Studies by Gill and Redden (2021) have also reinforced the view that this clarity is essential for protecting individual rights.

The Role of Public Trust in Cybersecurity Legislation

Lack of public trust badly impacts personal freedoms (Chan et al. 2022). According to Nyst (2016), citizens are more likely to support and comply with cybersecurity measures if they believe their rights are respected and protected. Therefore, lawmakers should strengthen national security efforts. International standards underscore the need for judicial oversight, clear legal definitions, and proportional limitations to avoid infringing on the fundamental rights. Insights from recent studies underline the need for legislative reforms that prioritize both security and civil liberties.

CONTROVERSIES OF DIGITAL SECURITY ACT 2018

A lot of disputations originated, in one way or another, from the moral grounds of the Act. Critics state that the law has been abused to restrict people's freedom of speech. Because section 57 of the ICT Act was retained in the legislation of 2023, albeit with certain revisions, the public felt that the law was more insecure. Defamation, hurting religious emotions, maintaining order, and inciting violence against any individual or group by publishing or disseminating any content via websites or electronic means were all included under Section 57.

It has punishment criteria in both fine sentences and imprisonment. Where prison punishment range starts from 10 years to 14 years. In certain situations, a police officer may search or detain a person without a warrant. Violation of DSA 2018 is considered 'non-bailable' crimes. Due to criticism that this section of the law is more harassing and prone to misuse, it has become even more notorious. A report by a renowned newspaper, The Business Standard expressed that 7001 DSA cases have been filed till January 31, 2023. The report also says that 80% of the cases filed by ruling party supporters against critics and opposition activities.

27.41% of cases have been filed against 355 journalists. A recent comparative analysis by Transparency International Bangladesh (TIB) has shown similarities between the DSA and the draft CSA. While the law of 2023 may carry a different name, key concerns regarding freedom of speech, dissent, and press freedom persist.

Additionally, a great deal of cases was brought against journalists, and several of them were detained under the DSA. As a result, a large number of journalists, NGOs, and civil society leaders spoke out against this Act and called for the DSA to be discontinued. Legislators have therefore ultimately prepared a new law titled Cyber Security Act, 2023 (CSA), which is thought to be the replacement for the DSA. The CSA considered the deficiencies of DSA.

Introducing The Cyber Security Act 2023

Initially the draft of the CSA was released on the ICT department's website on August 9, 2023. Within two weeks of its release, the stakeholders could review and comment on this draft. On August 28, 2023, the cabinet gave its final approval to the CSA draft after receiving and taking into account the opinions of the stakeholders. The Cyber Security Act 2023 got the approval

from the Honorable President of Bangladesh on September 18, 2023 and abolished the previous Digital Security Act 2018. The act has 60 sections. Among these, four sections are non-bailable. These are:

a. Section-17: Intrusion into important information infrastructures & others

b. Section-19: Damaging computers and computer systems

c. Section-27: Cyber terrorist acts and committing such crimes

d. Section-33: Hacking related crimes

IMPACT OF CYBER SECURITY ACT 2023 ON INDIVIDUAL RIGHTS

Comparison with Digital Security Act 2018

In defamation prosecutions brought under the Cyber Security Act 2023, which was just passed, monetary fines are imposed in lieu of jail time. In defamation situations, the police are not allowed to make an arrest (Section 29 of CSA 2023). The Cyber Security Act made certain offenses bailable that were non-bailable under the DSA. The new modifications have resulted in a shorter jail sentence for several offenders. The new version does away with the repeat offence punishment clauses.

A short comparison between Digital Security Act 2018 (DSA 2018) and Cyber Security Act 2023 (CSA 2023) has been shown below:

Offences	Penalties in DSA	Penalties in CSA
Section 21: Propaganda against the spirit of the Liberation war, the father of the nation, the national anthem or the national flag	10 year imprisonment or maximum fine of Tk. 1.00 crore	5 year imprisonment or Maximum fine of Tk. 1.00 Crore
Section 27: Committing Cyber Crime	14 year imprisonment or maximum fine of Tk. 1.00 crore	14 year imprisonment or maximum fine of Tk. 1.00 crore
Section 28: Offence of hurting religious sentiments	5 year imprisonment or maximum fine of Tk. 10.00 Lac	2 year imprisonment or maximum fine of Tk. 5.00 Lac
Section 29: Defamation in the context of news coverage	3 year imprisonment or maximum fine of Tk. 5.00 Lac	Maximum fine of Tk. 25 Lac
Section 31: Destroying communal harmony	7 year imprisonment or maximum fine of Tk. 5.00 Lac	5 year imprisonment or maximum fine of Tk. 25.00 Lac
Section 32 (CSA) /Section 34 (DSA) : Hacking	14 year imprisonment or maximum fine of Tk. 1.00 crore	14 year imprisonment or maximum fine of Tk. 1.00 crore

Data Removal or Blocking

Information that endangers public order or digital security may be blocked or removed under Section 08 of the Act. Although these measures may be necessary to deal with immediate

concerns, it is important to clarify the criteria and supervision procedures. To avoid censorship, it's also critical to make sure that the appeals procedure and decision-making process are transparent. Concerns are raised in this section about possible misuse, ambiguous terminology and possible effects on freedom of speech.

Vagueness and Potential Misuse

Vague phrases like "threat to digital security," "solidarity," "financial activities," and "religious values" are used in the Section 08. These phrases lack precise meanings, which leads to uncertainty and increases the possibility of sweeping interpretations by authorities. Due to its ambiguity, these laws may be abused to stifle free speech online and may result in arbitrary decision-making. The international human rights legislation orders to create objective rules for judging whether content genuinely endangers people or undermines solidarity.

Overbroad Restrictions on Expression

Section 25 of the Act criminalizes the publication or transmission of material that is insulting, false, or threatening. Section 28 makes it illegal to publish or transmit content that offends religious principles or sentiments. Although limiting harmful content is crucial, these clauses need to be carefully worded to prevent ambiguous language. International human rights legislation emphasizes that limitations on speech must be proportionate to a valid goal and precisely defined. Similar is also written in the International Covenant on Civil and Political Rights (ICCPR).

Criminalization of Online Activities

Certain parts of the law (Sections 17 and 18) criminalize conduct that may not be punishable by harsh criminal laws, such as gaining unauthorized access to computers, computer systems, or networks. According to best practices, punishments ought to be appropriate for the seriousness of the offense and shouldn't unduly restrict a person's rights. Legitimate online activities may be discouraged by overcriminalization.

Violation of the Right to Privacy

Section 24 of the Act deals with identity fraud or personation, whereas Section 26 deals with the unlawful gathering or use of identification information. The right to privacy should be taken into consideration when analyzing these requirements. In order to prevent abuse, the Act should guarantee that the definition of approved authority is made explicit. The acquisition and use of personal data should abide by recognized data protection rules.

Investigation and Powers

The Act's Sections (38–42) provide the Investigating Officer specific authority to look into cybercrimes, including the ability to search and seize digital devices. Although these powers are required for an efficient inquiry, it's critical to make sure they are used properly with accountability. Moreover, There should be precautions against potential abuse and clear guidelines for obtaining search warrants and carrying out searches. Regulations in Sections 41 and 42 continue to govern the authority for search, seizure, and arrest with and without a warrant as the previous DSA 2018. When there is probable cause that an offense has been or will be committed under the Act, Sect. 41 requires obtaining a warrant. The police investigator has unduly extensive powers under Sections 40, 45, and 46, which run the possibility of being abused. This worry is further compounded by the lack of oversight mechanism for the process of seizing computers and personal property. These clauses are characterized by a lack of exact definition and ambiguous criteria.

POSITIVE ASPECT AND NEGATIVE ASPECT

After all, we can classify our findings into two broad categories: Positive aspect and Negative aspect. The aspects are mentioned as below:

Positive aspects

The CSA aims to strengthen cyber security measures in Bangladesh. It also protects individuals and organizations from cyber threats. The CSA provides an opportunity to modernize the legal framework governing cyber security. Therefore, The establishment of the National Cyber Security Council under the CSA is helpful to minimize cyber threats effectively. The CSA confirms protection of critical information infrastructure is highly important.

Negative aspects

Provisions of criminalizing speech, hostile speech and defamation within cyber security law can lead to undue restriction on the right to freedom of expression. Some provisions of the CSA contain vague and broad language, committing to potential misuse and arbitrary enforcement. The CSA lacks sufficient judicial oversight concerning the powers granted to officers for seizure of digital devices.

Potential Misuse: The Context of Bangladesh

Ambiguities in law can create significant risks for overreach and misuse. In the case of Bangladesh's Cyber Security Act, certain provisions are noted as restrictions on individual freedoms (TIB, 2023). For instance, "threats to digital security" or "content harmful to public order," can be broadly interpreted because these are vague terminology. Research shows that when laws are ambiguous, they can easily be weaponized to suppress dissent or limit political opposition (Bigo et al., 2020). Furthermore, the lack of precise definitions makes it challenging to understand what constitutes an offense under the act. Individuals might avoid expressing opinions for fear of legal repercussions.

To mitigate these risks, robust institutional and judicial oversight is essential. A transparent oversight mechanism could help prevent misuse. Enforcement actions under the act are grounded in clear, consistent legal standards (Binns & Veale, 2020). This section emphasizes that institutional mechanisms, such as independent review boards or human rights councils, could enhance the accountability of cybersecurity enforcement in Bangladesh.

International Standards and the Need for Legal Reforms in Bangladesh

Bangladesh must align cybersecurity laws with international standards. We need a balance between protecting human rights and ensuring digital security. International laws does not accept restrictions on rights, including digital rights; restrictions must be lawful, necessary, and proportionate (United Nations, 1966). For Bangladesh to comply with these standards, legal and procedural reforms are necessary to make cybersecurity legislation more transparent, accountable.

Another critical area for reform is the adoption of specific guidelines that clarify the scope and limitations of cybersecurity enforcement. For example, laws in the European Union, such as the GDPR, incorporate clear guidelines on data privacy. GDPR enforces mechanisms are both transparent and strictly regulated (Baudot & Robson, 2017). Similarly, according to the United Nations cybersecurity laws should include safeguards against arbitrary surveillance and provide a clear, legal basis for any data collection activities (UN General Assembly, 2013). Reforms in Bangladesh's Cyber Security Act could include establishing independent bodies to oversee enforcement actions. Citizens have the right to accessible recourse mechanisms to challenge any unjust actions in the name of CSA. Furthermore, the ambiguous terms within the law would limit misuse by targeting only at genuine cyber threats (Akdeniz & Gillespie, 2019).

FUTURE RESEARCH

Future research could explore public perceptions of the Cyber Security Act 2023 over time. Comparative studies on the implementation and public reception of cybersecurity laws in

various countries, particularly within South Asia, could provide deeper insights. Additionally, longitudinal studies on the practical enforcement of the CSA 2023 would further contribute to understanding the balance between cybersecurity and individual rights.

CONCLUSION

In conclusion, alignment with international standards would support Bangladesh in developing a cybersecurity law. We must protect national interests without compromising individual freedoms. This section provides recommendations for legal and procedural reforms that could help Bangladesh create a balanced approach to cybersecurity governance. It can be said that the latest Cyber Security Act 2023 has both positive and negative sides. Considering these challenges, it is obvious that there is a pressing need for policymakers in Bangladesh to review and reform some sections mentioned in the Cyber Security Act 2023. Clarification of vague provisions will enhance transparency and accountability mechanisms and uphold international human rights standards. By adopting a rights-based approach to cybersecurity governance, Bangladesh can effectively address cyber threats. At the same time government will not fail to uphold the principles of democracy, rule of law, and respect for human rights.

REFERENCE

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics (Switzerland)*, 12(6). https://doi.org/10.3390/electronics12061333

Australia's Cyber Security Strategy 2020. (2020). Department of Home Affairs, Australia, 1–52. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf

Azad, A. (2021). *Digital Security Act in Bangladesh: The death of dissent and of freedom of expression* (Issue May). Central European University.

Bangladesh: Türk urges immediate suspension of Digital Security Act as media crackdown continues. (2023). https://www.ohchr.org/en/press-releases/2023/03/bangladesh-turk-urges-immediate-suspension-digital-security-act-media

Baudot, L., & Robson, K. (2017). Regulation. In *The Routledge Companion to Critical Accounting* (pp. 184–204). https://doi.org/10.4324/9781315775203-11

Bigo, D., Carrera, S., Guild, E., & Mitsilegas, V. (2020). *Controlling frontiers: Free movement into and within Europe*. Ashgate Publishing.

Binns, R., & Veale, M. (2020). Algorithmic accountability and privacy: Implications of AI in government surveillance. *Journal of Privacy and Surveillance Studies*, 15(4), 55–72.

Budiarto, M. K., Rahman, A., Asrowi, Gunarhadi, & Efendi, A. (2024). Proposing information and communication technology (ICT)-based learning transformation to create competitive human resources: A theoretical review. *Multidisciplinary Reviews*, 7(4). https://doi.org/10.31893/multirev.2024076

Cybersecurity Act 2018. (2018). *Republic of Singapore Government Gazette Acts Supplement* (Cybersecurity Act No.9 2018), 9, 72.

Cybersecurity Information Sharing Act of 2015. (2015). https://www.newamerica.org/oti/blog/cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/

De Hert, P., & Gutwirth, S. (2021). Data protection and the limits of the law: Challenges for privacy in the digital age. *Privacy & Security Studies*, 13(2), 101–121.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, 66(July), 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Federation, R. (2014). Federal Law No. 149-FZ of July 27, 2006, on information, information technologies, and protection of information (as amended up to Federal Law No. 222-FZ of July 21, 2014).

Government Gazette. (2021). Cybercrimes Act, 2020. Prevention, 672, 1–128. http://www.nsw.gov.au/sites/default/files/Government_Gazette_2_December.pdf#page=15

Government of the People's Republic of Bangladesh. (2019). Digital Security Act 2018 (Authentic English Text). 23319–23342. https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf

Govt alerts to stop misuse of Digital Security Act: Anisul Huq. (2023). https://www.kalerkantho.com/english/online/national/2023/03/22/51010

HM Government. (2022). *Government Cyber Security Strategy: 2022 to 2030*. UK Government, 1–78. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1049825/government-cyber-security-strategy.pdf

Indian Parliament. (2000). *The Information Technology Act*. https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

Lavorgna, A. (2000). Cyber-organised crime: A case of moral panic? *Trends in Organized Crime*, 22(4), 357–374. https://doi.org/10.1007/s12117-018-9342-y

MacKinnon, R. (2022). *Consent of the networked: The worldwide struggle for internet freedom*. Basic Books.

MCSS. (2020). *Malaysia Cyber Security Strategy 2020-2024*. Malaysia Cyber Security.

Nyst, C. (2016). *Travel guide to the digital world: Cybersecurity policy for human rights defenders*.

Pajuste, T., Čerkić, Š. M., Badurova, B., & Powell, C. (2022). Specific threats to human rights protection from the digital reality: International responses and recommendations.

Singh, D. (2023). Cybersecurity and human rights: A complex interplay. *International Journal of Science and Research (IJSR)*, 12(6), 1110–1112. https://doi.org/10.21275/sr23608234858

The Government of Japan. (2010). *The Government of Japan*. https://doi.org/10.4324/9780203841648

TIB. (2023). Prothom Alo. (Analysis on public trust concerns regarding Bangladesh's Cyber Security Act 2023).