DOI : https://www.doi.org/10.62673/JDIU.V13N1.A7 **ISSN : 2077-0111**

Rethinking Human Rights in the Digital Era: The Bangladesh Perspective

Dr. Abdullah-Al-Monzur Hussain[1]

Abstract: The rapid advancement of digital media has significantly impacted the understanding and application of human rights globally, including in Bangladesh. This study explores the interplay between human rights and digital media, emphasizing challenges such as privacy breaches, online harassment, censorship, and surveillance. Additionally, it examines opportunities for enhancing freedom of expression, access to information, and safeguarding democratic values. By analyzing the legal frameworks and societal implications in the Bangladeshi context, the research highlights critical gaps in protecting digital rights and proposes a collaborative, rights-based approach to addressing these challenges. The findings underscore the need for updated policies, public awareness, and multi-stakeholder engagement to uphold human rights in the digital age.

Keywords: Human rights, digital media, Bangladesh, privacy, freedom of expression

Introduction

The rapid convergence of physical, digital, and biological worlds has transformed how individuals and societies interact, innovate, and thrive. This digital transformation is more profound than the invention of writing or printing, reshaping fundamental aspects of human life and communication. In the digital era, where virtual interactions often overshadow face-to-face connections, the boundaries between public and private spheres have blurred. These changes have significant implications for human rights, particularly in the domains of freedom of expression, privacy, and access to information. Bangladesh, like many other nations, is navigating the opportunities and challenges of digital innovation. While digital platforms offer unprecedented possibilities for empowering citizens and enhancing governance, they also pose risks, including online harassment, surveillance, censorship, and data misuse. As the nation strives to establish "Digital Bangladesh," questions arise about the adequacy of existing legal frameworks in protecting human rights in the digital context. This paper examines the interplay between human rights and digital media in Bangladesh, focusing on critical issues such as privacy, freedom of expression, and the ethical use of technology. By exploring the legal and societal dimensions of these challenges, it seeks to propose actionable solutions for fostering a balance between technological advancement and human rights protection.

[1] Associate Professor & Head, Department of Law, Prime University, Dhaka.

Objectives

The study aims to examine the evolving dynamics of human rights in the context of digital media, with a focus on the unique challenges and opportunities within Bangladesh. The specific objectives are as follows:

1. To critically analyze the implications of digital media on the traditional understanding of human rights, including privacy, freedom of expression, and access to information.
2. To evaluate the effectiveness of Bangladesh's legal frameworks in addressing human rights issues arising in the digital sphere.
3. To explore the intersection of digital media and governance, particularly in safeguarding democratic values and citizen empowerment in Bangladesh.
4. To propose actionable recommendations for strengthening human rights governance in the digital age, inspired by international best practices and local needs.

Methodology

This study employs a mixed-method approach, incorporating qualitative and descriptive methods to examine human rights in Bangladesh's digital context. Primary sources include constitutional documents, statutory laws, international human rights instruments, and case studies highlighting critical incidents. Secondary sources comprise academic literature, government reports, and media analyses to provide theoretical and contextual insights. Data collection involved reviewing digital platforms, social media, and expert opinions to capture real-time trends. Thematic and comparative analyses were conducted to identify patterns and evaluate Bangladesh's policies against international best practices. This comprehensive approach ensures a nuanced understanding of the challenges and opportunities within the digital sphere.

Revisiting Human Rights in the Digital Context

The phrase digital rights represent human rights like getting, using, making, and distributing digital media or accessing and utilizing PCs, other electronic gadgets, or communications networks. This term is especially exercised to protect and acknowledge existing rights, such as the right of privacy or freedom of expression, with regards to new technologies, particularly the Internet. Get Internet access is perceived as a right by the laws of several countries. (Ahamuduzzaman, 2015, 184) The digitization of public discourse in Bangladesh has led to a cultural shift, where citizens increasingly rely on digital platforms for news, education, and community engagement. However, this shift has also exposed deep inequalities in access and digital literacy, posing barriers to inclusive digital rights. Social media platforms have become vital tools for grassroots activism in Bangladesh. Movements like the road safety protests of 2018 demonstrated the power of digital platforms in mobilizing citizens and amplifying

their voices globally. However, these platforms have also been weaponized for misinformation and targeted harassment.

Right to Speech in the Digital Media

A free and open web is the foundation of a cutting-edge way to deal with human rights. Digital technology has made a scope of new ways for individuals to communicate their perspectives and draw in with a public discussion about the eventual fate of our general public. We look to secure this progression and discover approaches to make life online comprehensive. Protection of digital rights supports national and international online mediators and social networking platforms to ensure the right of Freedom of speech by giving good and successful instruments to restrict and address maltreatment on their networks. The internet, an extraordinary potential, has worked with a type of democratization of broadcasting and public commitment. Yet, this is just possible if we make sure of setting up the securities for the discourse to be allowed. The new methodologies are required for people to make the development of the stages strong to communicate their thoughts and work using the internet. Additionally, Freedom of speech implies that people can raise their voice by fear or any assessment. With the ascent of social media, independent publishing, blogs, and other open media, there are new and complex issues about who is obligated to monitor the discourses online. We should guarantee that digital platforms are planned in manners that promote human rights and the commitments for partnerships for ensuring weak individuals in their terms of administration, how their principles are authorized, and the specialized plan of their frameworks. Most importantly, choices about which components of discourse are worthy should be made in a manner that is reasonable and responsible to stay away from restriction. The long-term conversation will involve this among the government, the corporations, and the civil society as it is a growing and developing sector getting it right.

It perceives the administrations that may confine the right of freedom of expression where it is a vital proportion to confirm the public safety, public appeal, and other privileges. The present sadness is that we are getting experiences about the global assault on freedom of expression. Throughout the world, the governments are lengthening the importance of what's allowed: They characterize national security widely imposing the indefinite ways that make it hard for people to know what discourse or conclusions are permitted and what might be dependent upon punishment, they apply the restrictions that worked out positively past what is important to be addressed, and they mistreat to legitimize their limitations. We get this incident, especially in the digital era, like limiting the freedom on media and assaulting the civil society. The internet and digital communicative technology bring to light the difficulties for the freedom of expression; however, they are similar issues that we have found since the enacted human rights law. Governments are attempting to limit the progression of data brace down on analysis and monitor residents. The digital age gives

striking admittance to getting new information and ideas, and we regularly unwittingly expect to protect our privacy and personal information to governments and organizations. The thing is going at this point as we just read the newspaper; the newspaper will read us. One model is identified with the opportunity to keep up with sentiments without impedance. There is limited understanding around this right because the writers of Article 19 probably accepted the option to hold an assessment is undeniable—governments cannot get what is in our minds. Nevertheless, we now a day carefully stock such a great deal of what is to us under the cloud, in our laptops and our local servers, the very places subject to be protected and surveillance by governments. Concerning privacy regarding the data accessible, online will prompt an absence of information sharing on digital platforms and self-censorship. (Rahman, 2016, 118)

Right to Internet Access

Many human rights have been enacted to address digital security concerns and safeguard fundamental principles such as freedom of expression, privacy, freedom of association, and data protection (United Nations, 1948; United Nations, 1966). Countries like Estonia have pioneered initiatives to make internet access a fundamental right. In contrast, Bangladesh still grapples with infrastructural limitations and unequal internet penetration, particularly in rural areas, which perpetuates the digital divide. In addition, the right to education, multilingualism, consumer rights, and capacity building have also been recognized as essential aspects of digital rights (United Nations, 1948; United Nations, 1966). The Internet, being a global public resource, should be accessible to all while respecting the rights of others (United Nations, 2016). As of 2023, approximately 47% of Bangladesh's population has internet access, with significant disparities between urban and rural areas. (World Population Review, 2023) This digital divide limits marginalized groups' ability to exercise their digital rights, including access to education and information. However, in the face of restrictive systems that limit access to information and communication, democratic governments should strive to ensure Internet access and uphold universal principles to ensure a secure and inclusive network (United Nations, 2016).

Data Privacy and Human Rights

In this time of data and correspondence innovation, "data" has gotten the new dash for unheard of wealth for both state entertainers (governments, law requirement offices, knowledge, and so on) and non-state entertainers (enterprises, worldwide organizations, singular programmers, or programmer gatherings, fear monger associations, and so forth). In the case of controlling social movements, tactical security, elevation, and marketing of products, retaining public order, charting development policies, preventing crimes, etc., Personal Data has been a vital fact. Our information is continually gathered, duplicated, put away, and handled by the state and non-state entertainers (referenced as "others" from this point forward) as per their demand. The increasing use of AI-driven systems in Bangladesh, such as biometric

databases and automated surveillance, raises concerns about data privacy and consent. Without robust data protection laws, citizens remain vulnerable to breaches and misuse of sensitive information. We don't generally get the admittance and the ownership. That's why the personal data at present has been turned to be the "holy grail" of "Big Data." Big Data is considered as an enormously enormous size of information containing all the information that might be found on the internet and gathered through the Internet of Things (IoT) (any digital device connected to the internet, such as smart-watch, smart TV, mobile phone, CCTV camera, GPS, computer, etc.).

The collection of personal data has profound implications for our privacy, behavior, vulnerability to misinformation, digital divide, and the perpetuation of bias and segregation (Smith, 2022). It also subjects us to the control of powerful entities that benefit from data, altering societal values, ethics, and cultures. When the state possesses our data, the situation worsens as it is collected under legal provisions that grant advantages to the state, leaving citizens with limited recourse to challenge lawful data collection orders (Smith, 2022). Moreover, this data is scrutinized by Artificial Intelligence (AI) systems to create profiles based on assumptions about individuals' behaviors, characteristics, preferences, movements, social interactions, lifestyles, and more. This raise concerns as AI algorithms have been criticized for fostering discrimination and racism, exemplified by instances of anti-Semitism and price discrimination based on location (Smith, 2022). AI algorithms manipulate us, transforming us into passive and programmable individuals who willingly provide personal data without questioning the ethical implications, thereby reducing resistance (Smith, 2022).

With regards to Bangladesh, we need tech-neutral laws which will be equipped for synchronization with ICT changes. Bangladesh currently lacks a comprehensive data protection law, leaving citizens' digital identities unprotected. (Data Reportal, 2023) This absence highlights an urgent need for legislation that aligns with international standards, such as the GDPR. In addition, we direly need a specific data protection law. These laws need to recognize that all the fundamental constitutional rights ensured offline must be protected online. The meaning of "privacy" must be refreshed in our Constitution by data protection. Alongside this load of laws, our ICT arrangements should likewise recognize that data protection is a central component of our right to privacy which at last reinforces the democratic values of society. Most importantly, we individuals should comprehend that our data belongs to us, not anyone else.

Cyber Security and Human Rights

The discussants in the public discussion on securing digital context have emphasized the need to balance privacy and other human rights with the objective of maintaining public security (Smith, 2019). However, it is important to recognize that excessively prioritizing privacy and human rights may pose risks to public safety. Framing privacy and human rights as conflicting with public safety and national security not only lacks

substance but also undermines freedom and security (Smith, 2019). To address this, it is crucial to integrate the concept of public safety and national security into existing cybersecurity policies in order to strike a balance (Jones, 2020). Given the increasing frequency and complexity of cyber threats and cybercrime, all stakeholders must collaborate to develop measures that preserve human rights, particularly freedom of expression and privacy (Jones, 2020). The "An Internet Free and Secure" act focuses on safeguarding individual security, which serves as a driving force behind cybersecurity and ensures the protection of human rights in the digital context (Smith, 2019).

As Cyber security and human rights are mutually associated, both should be required to ensure the freedom and security advance. Identifying the individual security at the center of network safety implies the assurance for human rights that ought to be at the focal point of developing a cyber-security policy. The policy-makers of the cyber security policy should particularize between Digital security and human rights reflecting by design. (Rahman, 2016, 48)

Bangladesh's experience of Human Rights in the Digital Context

Recently, there has been a temporary expansion of cyberspace in Bangladesh; however, there have also been efforts to stifle free expression and speech related to cybersecurity (Kabir, 2019). Several bloggers and cyber activists have been brutally murdered, leading many others to leave the country out of fear of further attacks. Despite the risks, the internet remains vibrant, and young people continue to express their opinions on various public issues (ibid). Instances such as the use of the ICT Act to silence writer Prabir Sikder and the arrest of Dilip Roy for his Facebook post demonstrate how the authorities have employed peculiar charges to restrict free speech (ibid). The government's intervention against bloggers aligned with Hefazat-e-Islam using Section 57 of the ICT Act serves as another example of suppressing dissent (ibid). While the Act has been revised and certain changes have been introduced to Section 57, a critical analysis reveals that the revised provisions are essentially the same as before, with only minor adjustments (ibid). These incidents have eroded people's confidence in the Digital Security Act, and if it continues to be enforced, it will further restrict freedom of expression on digital platforms (ibid).

Revisiting Existing Cyber Laws of Bangladesh

The Digital Security Act, 2018, planned to address the requirement for digital wrongdoing enactment, as indicated by the specialists, was supported in January 2018 by the Cabinet. So far, individuals from media, activists, and society have effectually communicated their interests over the law imposing upon the individuals' free scopes of vocalization. Our constitution confirms "the right of every citizen to freedom of speech and expression" as a fundamental right. The Digital Security Act, 2018, may illogically reject this right, limiting basic reason, analyzing the norm, and snatching from people one of their most notable weapons; the right to talk unconditionally and

freely. The worrying matter is that the Digital Security Act, 2018 is with its well-established setting and its weak content. The existing ICT Act is not all-embracing and customary laws that have not any reasonable option for its further advance. Online purposeful publicity by worldwide psychological oppressor associations and late Bangladesh Bank heist just reinstated the threat of cybercrime that can encounter the geopolitical limits and customary safety efforts. As unsatisfied with it, the Law Minister said that the law would reset to erase all the debates over Section 57 of the ICT Act. However, Section 57 got injected into sections 19 and 20 of the new law. Subsequently, all the disagreements with the Section 57 will stand valid against the new advanced security law. Rather than drafting another law, the experts could mark the ICT Act more extensive. The term 'digital' may produce good sound with a comprehensive mood than ICT.

Section 57 of the ICT Act is a genuine danger to independent people and has many challenges. It was additionally censured in various public and global discussions. Rather than canceling this harsh law, the public has wanted to dispatch the Digital Security Act, which will also fix the noose on free reasoning. As per the public authority, the new Act will assist with checking any endeavor to depict our Liberation War and Bangabandhu contrarily in the computerized space. In any case, they have failed to remember that digital activists assumed a vital part in getting sorted out the Shahbagh uprising, which was a colossal dissent against hostile to the Liberation War components. So this endeavor to choke any basic voice in the digital circle for the sake of maintaining the soul of the Liberation War is self-opposing. People fear this law, like the ICT Act, that may transform into an abusive law. The greater portion of the cases under the ICT Act had been drifted under Section 57, even though some different offenses were referenced there. The proposed law offers scope for silencing individuals' voices. Definitions are not explicit, and numerous abusive measures have been supported under the wide umbrella of public safety (Alam, 2014, 236).

Bangladesh has instituted the Information and Communicating Technology Act, 2006 interestingly to cover every one of the issues regarding advanced, virtual, or Electronic Media. By this Act, Bangladesh has ordered the primary law in regards to ICT matters. However, this law sets out enormous freedom to give a structure to direct every one of the issues in this area. Albeit the law has been attempting to give a rule and control every one of the actions in such a manner, a few arrangements of the law become the sword of the decision gathering to go against the voice of individuals, writers, and others. In this regard, the law is needed to be refreshed or revised for the prerequisite of the percent time. In any case, disregarding making change, the public authority has drafted another law in 2018 named Digital Security Act, 2018. This law is presently under an incredible analysis of the general public's different levels for numerous reasons.

The scope of the articulation was put to the cutting edge, feared writers and rights of safeguards as the bureau validated the Digital Security Act, 2018.(The Diplomat, 2023) Each opportunity of the Act would have abused against individuals' all in all correct to communicate them after being passed by the Parliament. They likewise sensed trapped by the public authority as Section 57 of the Information and Communication Technology Act which had been kept in the proposed law due to the assured changes. Section 57 provisions with harming strict estimations, criticism, causing crumbling of the rule of law and warning against any individual or association through distributing or sending any material in online sites or platforms. It identifies the highest 14 years in jail for the offenses. There are four separate sections of the Digital Security Act, 2018 for the offenses with a discipline going to jail from three to 10 years' term. The law depicts a few violations as "non-bailable" and permits a police officer to look or capture anybody without a warrant in unique conditions (Haque, 2015, 331).

The Digital Security Act, 2018 has contained an arrangement for renouncing sections 54, 55, 56, 57, and 66 of the ICT Act, and the cases previously recorded under section 57 will proceed. As of now, very nearly 701 cases documented under section 57 are forthcoming with the solitary digital court of the country. The activists and writers have been requesting the abolition of section 57 for its widespread mistreatment. Experts recommended correcting the conflicting part with individuals for ensuring the opportunity of articulation freely and freeing discourse because it contains questioning phrasings, permitting its abuse against newscasters and online media clients. Fights were organized last year after more than two dozen writers were sued under the part. We have been requesting the undoing of section 57. However, the things have not been enhanced; rather, more awful apparatuses have been presented. The Act won't just control the ability to talk without any fear and articulation yet, in addition, obstructs the autonomous news-casting.

The inclusion of section 57 in the Digital Security Act of 2018 raises concerns about the potential misuse of the law to suppress freedom of the press (Haque, 2020). If the draft law is passed as it stands, it could provide a loophole for using section 57 to harass individuals, similar to previous instances (Haque, 2020). The implementation of the Digital Security Act will likely lead to a reduction in freedom of expression, closing off avenues for discussion on specific topics and limiting free speech (Haque, 2020). It is crucial to have provisions within the Act that require authorities to conduct proper investigations before taking action on offenses or alleged offenses related to religious sentiments (Haque, 2020). The proposed changes to the law reflect the government's inclination towards restricting freedom of expression, exposing its undemocratic nature (Haque, 2020).

Major Lacuna of Cyber Laws of Bangladesh

Some significant weaknesses and insufficiencies which are making open bar to guarantee digital security alongside human rights approaches are mentioned under:

- ✓ The law clashes with international guidelines that Bangladesh is a signatory to Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR). It even negates with Article 39 of the Constitution of the People's Republic of Bangladesh.
- ✓ The Digital Security Act, 2018, has been made in Bangla, which is for the comfort of individuals. Be that as it may, the meanings of the different legitimate and specialized viewpoints given in Section 2 are a curious combination of Bangla and English, which individuals without specialized mastery won't comprehend.
- ✓ There are likewise issues with due respect to the wrongdoings and disciplines referenced in the law. Criminal law should be explicit. In the new Act, the wrongdoings are not characterized. It gives scope for irregular provocation of individuals. The sentences characterized in the law are additionally unbalanced and don't consider the expectation of the denounced.
- ✓ Section 13 of the law is exceptionally vague and sweeping. Its freedom of speech with the excuse of national security. It implies that I would not have the option to protest the Rampal Power Plant since it may jeopardize relations with a friendly country.
- ✓ It will condemn online works through ambiguous terms and shrink space for a scholarly talk by advancing self-censorship. The way Sections 15(4) (5) of the new law condemns compositions against Bangladesh's foreign policy, Bangabandhu, and liberation war implies space for maltreatment of it in some wrong hands.
- ✓ Section 15(4) boycotts work against Bangladesh's foreign policy, although Bangladesh doesn't have any freely distributed international strategy except for a couple of lines in the Constitution. If the foreign policy conflicts with our fundamental principles, for what reason would it be advisable for us not to revolt against it? We know without a doubt that even the Awami League and the Bangladesh Nationalist Party have various takes on our foreign policy.
- ✓ In 1971, numerous Americans went against the authority position of the United States to help Bangladesh's freedom war. How might we presently uphold Section 15(4) that conflicts with that soul of 1971? Indeed, even to carry out Banganbandhu's dreams, his works and strategies need to go through research and, frequently, valuable analysis. Additionally, even with our feeling on liberation war history, we should participate in worldwide scholarly discussions with proof and arguments.

- ✓ Section 19 also is loaded with dubious definitions. Who characterizes immoral? The state isn't there to do moral policing. Sections 295-298 of the Bangladesh Penal Code as of now cover issues about hurting religious sentiments.
- ✓ There are likewise inner contentions in the law. Section 37, which is practically equivalent to Section 71 of the ICT Act, says an appointed authority won't give bail on the off chance that he is persuaded that the blame of the charged isn't intense. It is a presupposition of guilt. The judge has effectively taken his view before preliminary, which sabotages the principle of law.
- ✓ The law additionally gives police of the examiner rank the ability to explore these crimes. Do they have ICT training? We don't have a Digital Evidence Procurement Policy for an assortment of digital evidence. In developed countries, the evidence is collected in front of the accused, and two duplicates are produced. A duplicate is served to the accused, and a signature is taken. Only then can the evidence be utilized in court.
- ✓ The law additionally proposed the making of a Digital Security Agency. The BTRC is the fundamental administrative body of the ICT law, and there is no requirement for another agency. The power is given to the agency under the new law is sweeping and contradictory with existing laws.
- ✓ The law gives the Director-General of the new agency the power to take punitive measures. Why is the Director-General acting as the court when the trial is supposed to occur under the ICT Tribunal (Hossain, 2015, 521).

Recommendations for Cyber Security Policies, Laws and Digital Rights

- ✓ Cyber security policies and decision-making processes ought to ensure and regard human rights.
- ✓ The improvement of cybersecurity-related laws, arrangements, and practices ought to, from their initiation, be human rights regarding by design. Cyber security-related laws,
- ✓ approaches, and practices should improve the security of people online and offline, thinking about the lopsided dangers looked at by individuals and groups at risk.
- ✓ The improvement and execution of cybersecurity-related laws, strategies, and practices should be associated with international human rights law, international law, and humanitarian law.
- ✓ Cyber security laws should not be practiced in violating human rights like association, assembly, free expression, and privacy.
- ✓ Responding to cyber-related incidents should not interrupt human rights.

- ✓ Any policies and practices related to Cyber security laws should endorse and guard the solidity and safety of the Internet. They should not hamper the integrity of infrastructure, software, hardware, and services.
- ✓ Cyber security-related laws, approaches, and practices ought to mirror the critical part of encryption and secrecy in empowering human rights activity, particularly free expression, association, assembly, and privacy.
- ✓ Cyber security-related laws, approaches, and practices ought not to hinder technological developments that contribute to the protection of human rights.
- ✓ Cyber security-related laws, policies, and practices at national, regional, and international levels ought to be generated using inclusive and transparent approaches with the involvement of all stakeholders.
- ✓ Stakeholders ought to promote education, digital literacy, technical and legal training to improve cyber security and the realization of human rights.
- ✓ Human rights regarding cyber security best practices ought to be shared and advanced among all stakeholders.
- ✓ Cyber security capacity building has a significant part in improving people's online and offline security; such endeavors ought to advance human rights regarding ways to deal with cyber security.
- ✓ Women in Bangladesh face disproportionate risks in digital spaces, including online harassment and cyberbullying. This underscores the need for gender-sensitive digital policies to protect vulnerable groups.

Conclusion

In an era where digital technologies permeate every aspect of human life, the intersection of digital media and human rights demands urgent attention. This study highlights the profound impact of digital platforms on traditional human rights concepts, particularly in the Bangladeshi context, where both opportunities and challenges coexist. While digital media fosters freedom of expression and democratizes access to information, it also exposes vulnerabilities, such as data privacy breaches, online harassment, and censorship. Bangladesh's journey toward "Digital Bangladesh" presents a critical case for understanding how emerging technologies intersect with governance and societal values. The study underscores the gaps in existing legal frameworks, which often fail to balance the protection of individual rights with the need for security and innovation. Without comprehensive policies and updated legislation that prioritize digital inclusion, transparency, and accountability, these gaps may widen, leaving citizens exposed to systemic vulnerabilities.

This research calls for a multi-stakeholder approach to ensure the safeguarding of human rights in the digital age. Policymakers, civil society, and technology companies

must work collaboratively to address challenges, promote digital literacy, and strengthen governance structures. Drawing from international best practices, Bangladesh can establish a robust framework that protects digital rights while fostering innovation and growth. Ultimately, as the digital transformation reshapes societies, the commitment to a rights-based approach is essential. By ensuring that human rights principles extend seamlessly into the digital realm, Bangladesh can navigate this new era while upholding democratic values and empowering its citizens in an increasingly interconnected world.

References

1. Ahamuduzzaman. (2015). *International human rights law*. Dhaka: Shams Publications.
2. Alam, M. S. (2014). *Enforcement of human rights law in domestic court*. Dhaka: CSB Publications Limited.
3. Data Reportal. (2023, February 8). *Digital 2023: Bangladesh*. Retrieved from https://datareportal.com/reports/digital-2023-bangladesh
4. Faruqque, A. Al. (2012). *International human rights law: Protection mechanism & contemporary issue*. Dhaka: New Warsi Book Corporation.
5. Haque, Z. (2015). *Laws and regulations of telecommunication services in Bangladesh*. Dhaka: B. S. T.N. Publications.
6. Henry, J. S. (1996). *International human rights in context*. Oxford: Clarendon Press.
7. Hossain, Md. F. (2015). *Telecommunication laws of Bangladesh*. Dhaka: University Publication Limited.
8. Jones, A. (2020). Cybersecurity, human rights, and the digital age. *Journal of Cyber Policy, 5*(2), 209-224. https://doi.org/10.1080/23738871.2020.1729795
9. Kabir, A. H. M. A. (2019). Freedom of expression and cybersecurity: A study on the situation of Bangladesh. *Digital Studies, 10*(2), 155-166.
10. Malik, T. (1997). *Manual on human rights law*. Dhaka: Bangladesh Bar Council.
11. Rehman, J. (2003). *International human rights law: A practical approach*. Essex: Pearson Education.
12. Smith, J. (2022). The impact of personal data collection on privacy and society. *Journal of Privacy and Data Protection, 10*(1), 45-62.
13. Smith, K. M. R. (2007). *International human rights* (3rd ed.). Oxford: Oxford University Press.
14. The Diplomat. (2023, August 9). *Bangladesh government scraps controversial Digital Security Act*. Retrieved from https://thediplomat.com/2023/08/bangladesh-government-scraps-controversial-digital-security-act/
15. United Nations. (1948). *Universal declaration of human rights*. Retrieved from https://www.un.org/en/universal-declaration-human-rights/

16. United Nations. (1966). *International covenant on civil and political rights*. Retrieved from https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
17. United Nations. (2016). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Retrieved from https://undocs.org/A/HRC/32/38
18. World Population Review. (2023). *Internet Penetration by Country 2023*. Retrieved from https://worldpopulationreview.com/country-rankings/internet-penetration-by-country
19. Zamir, M. (1990). *Human rights issues & international law*. Dhaka: University Press Limited.