The Major Role of Cyber Law in Ensuring Privacy of Netizens: A Case Study of Bangladesh Perspective

Md. Ashikur Rahaman Tareq[1], Most. Moklesunnahar[2], Dr. Md. Shahidul Islam[3]

[1]Department of Law and Justice, Bangladesh Army University of Engineering & Technology, Natore-6431, Bangladesh.

[2]Lecturer, Department of Law and Justice, Bangladesh Army University of Engineering & Technology, Natore-6431, Bangladesh.

[3] Professor, Department of Law and Justice, Bangladesh Army University of Engineering & Technology, Natore-6431, Bangladesh.

DOI: https://doi.org/10.51244/IJRSI.2024.1108018

Received: 15 August 2024; Accepted: 22 August 2024; Published: 30 August 2024

ABSTRACT

This article is based on cyber-crime and legal analysis only. To know about cyber-crime and types of cyber-crime, cause for cyber-crime, actual role of cyber law in ensuring privacy of netizens, Which laws and regulations were in place to stop the cyber-crimes included in this article. This research article focuses on the privacy of netizens and restraint all cyber related crime according to provisions of Bangladesh. While Bangladesh have The Information and Communication Technology Act, 2006; The Pornography Control Act, 2012; The Cyber Security Act, 2023; Bangladesh Telecommunication Regulatory Commission Act, 2001; provisions that is for cyber-crime.

Apart from that, other general provisions like, Cyber Jurisdiction; The Constitution of the People's Republic of Bangladesh, Bangladesh Penal Code, 1860, Copyright Act, 2005; is also included as a case analytical study. In this study, many famous case references of Bangladesh are included as case studies of cyber-crime which sets a precedent in cyber-crime control. Besides, some challenges of the government in implementing cyber-crime have been highlighted in this article**.**

INTRODUCTION

In today's digital age, the internet has become an integral part of our daily lives, transforming the way we communicate, work, and interact with the world. With the vast amount of personal information shared online, the need to protect individuals' privacy has become paramount. Cyber law plays a crucial role in safeguarding the privacy of netizens by establishing regulations and legal frameworks that govern the use of the internet and the protection of sensitive data. Cyber law plays a vital role in ensuring the privacy of netizens in Bangladesh by providing legal frameworks for the protection of personal data, regulating online activities, and addressing cyber-crimes. These laws help safeguard individuals' privacy rights, ensure data protection, and prosecute those who violate online privacy. In Bangladesh, the Digital Security Act of 2018 addresses various aspects of cyber-crime and provides provisions for the protection of privacy and data security. Additionally, it's important for these laws to be regularly updated to address new technological developments and emerging threats to privacy in cyberspace.[1]

Statement of Problem

The problem statement in this study should give a thorough summary of the specific issue or problem related to cyber-crime. The ease of internet access is the main problem that contributes to cyber-based crimes. Millions of individuals are suffering from it and having their lives harmed. Many of them suffer significant injuries as a result of cyber-crime. I also learned from my research that adults and kids make up the bulk of cyber-crime victims. The younger generation is being severely impacted by several issues, including pornographic websites,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

the availability of illegal substances, unauthorized access, etc. These issues are making them more curious about illegal matters they shouldn't be aware of, which in turn leads them to commit crimes out of curiosity.

CYBER-CRIME

Including a range of illegal actions carried out online, cyber-crime represents a substantial problem for Bangladesh. Cyber-bullying, online fraud, identity theft, hacking, and the spread of malicious content are examples of common cyber-crimes. Strong regulatory measures are required to discourage offenders and protect digital assets, since the spread of social media platforms and digital financial services has increased the scope of cyber-crime.

Cyber-crimes provide serious obstacles for Bangladeshi citizens, companies, and the government. These crimes cover a broad spectrum of illegal actions carried out via digital platforms, such as identity theft, online fraud, cyber bullying, hacking, and the distribution of harmful content. The prevalence of cyber-crimes highlights how crucial it is to have strong legal frameworks and law enforcement to properly counter these threats. The ICT Act of Bangladesh identifies different types of cyber-crimes and lays forth punishments for violators. Furthermore, the government assigned specific sections within law enforcement agencies the responsibility of looking into and prosecuting cyber criminals. Nevertheless, in spite of these initiatives, cyber-crimes persist and require ongoing modifications to legal frameworks and law enforcement tactics in order to remain ahead of their perpetrators.[2]

Causes for Cyber Crime

Modern technology is slowly increasing the number of cyber threats, and these attacks can sometimes be unpredictable.

The main factors contributing to cyber-crime and cyber-vulnerability are as follows:

1. Lack of schooling and illiteracy
2. Private information is online
3. A relatively small amount of data storage space
4. Inadequate operating system and negligence

DIFFERENT RIGHTS GUARANTEED AS CYBER RIGHTS

(a) Right to Pluralistic Media

Customers are entitled to a diverse range of media. Gaining a deeper comprehension of the threat industry consolidations pose to the open Internet, particularly how dominating Internet companies use their position in one market sector to stifle competition in other market sectors, is imperative for both governments and Internet users.[3]

The concepts of digital freedom, privacy, information access, and protection from online damage are often at the centre of the rights of netizens, also referred to as internet users or citizens of the internet. Here are some essential details about netizens' rights.

(b) Freedom of Expression: Users of the internet have the freedom to express themselves, including the freedom to exchange thoughts, ideas, and information without fear of reprisal or restriction. Freedom of expression is defined as a right that should be granted to every human being on the earth in Article 19 of the United Nations Universal Declaration of Human Rights. The freedom to hold beliefs without hindrance and the ability to seek, receive, and disseminate information and ideas through any media and across all boundaries are fundamental rights that every person has. According to the Universal Declaration of Human Rights, n.d.[4]

(c) Right to Privacy and Data Protection: Internet users have the right to privacy. This covers the freedom to manage their private data, the right to private correspondence, and defence against unauthorized monitoring or data gathering.[5]

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

(d) Access to Information: Internet users are entitled to use any information and knowledge that is publicly accessible on the network without any limitations from businesses or governments.

Information access is important and recognized as a fundamental human right by the United Nations Human Rights Council (UNHRC). Particularly, as stated in Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[6] and the Universal Declaration of Human Rights (UDHR), the right to access information falls under the larger category of the freedom of expression. The UNHRC's acknowledgement of information access confers legal value upon it as follows:

1. The Universal Declaration of Human Rights (UDHR): The UDHR explains the access of right to information is a module of the freedom of expression. The UDHR also states that the right to freedom of opinion and expression has been guaranteed for every human being. This right includes freedom to embrace opinions without interference and to seek, receive and impart information and ideas through any media and regardless of edges.[7]

2. The International Covenant on Civil and Political Rights (ICCPR) is the internationally enforceable Convention on Civil and Political Rights (ICCPR), which went into effect in 1976, safeguards a variety of civil and political rights, including the freedom of speech. The language of the Covenant which upholds the freedom to seek, receive, and disseminate information and ideas of all types, is identical to that of Article 19 of the UDHR.[8]

3. UNHRC Reports and Resolutions: The UNHRC consistently adopts reports and resolutions highlighting the significance of information access as a human right. These resolutions frequently urge states to uphold and advance the right to free speech, among other things by guaranteeing information access and battling censorship.[9]

4. The UNHRC, in collaboration with other UN entities including the Office of the High Commissioner for Human Rights (OHCHR), is tasked with monitoring and reporting on the state of human rights in various nations across the globe. These procedures could deal with infringements on the right to information access and offer suggestions for enhancements.[10]

(e) Freedom of Press: This is mentioned in Bangladesh and is governed by the Constitution of the People's Republic of Bangladesh as (a) the right of every citizen to freedom of speech and expression, and (b) freedom of the press are guaranteed. Press freedom is guaranteed by the constitution, as is to be anticipated; nonetheless, the problem arises when this provision is subject to certain restrictions.[11]

(f) Right to Digital Security: Netizens' right to digital security is increasingly recognized by international organizations such as the United Nations, which promotes digital rights and privacy safeguards in a variety of declarations, resolutions, and conventions. Organizations such as the International Telecommunication Union (ITU) and the United Nations Educational, Scientific, and Cultural Organization (UNESCO) seek to protect digital rights and promote cyber-security measures on a worldwide scale.

ITU regularly organises cyber-drills at the national and regional levels to build capacity and enhance technical collaboration between and within nations in order to improve incident response and management skills. ITU has carried out more than 30 cyber-drills involving more than 100 nations thus far.[12]

(g) Copyright and Fair Use: The legal idea of copyright states that all creative works, including music, photographs, literature, and art, belong to the individuals who created them. Any creative material you produce and record in a permanent format is your own intellectual property, as defined by copyright laws. This implies that someone else cannot lawfully steal your work and pass it off as their own. They are also unable to profit from the goods you produce. Even items that are protected by copyright may nevertheless be cited and referred to in your writing. However, you must have the owner of the copyright's consent in order to use, copy, or alter a work that is protected by a copyright. We refer to this authorization as a licence. While everyone has the right to demand that others respect their copyright and obtain permission before using their work, some individuals and businesses decide to provide more liberal licences for their content. They accomplish this by releasing their

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

creations under a creative commons licence or putting them in the public domain.[13]

As per the provisions of Bangladesh constitution, every internet user is entitled to copyright and fair use of any intellectual property. A crucial right for internet users is this one. In the meta-verse or online realm, individuals possess ownership over their intellectual property, just like they do in the physical world. Actually The rights mentioned above can be exercised by a netizen'.[14]

CYBER JURISDICTION IN BANGLADESH

Governance means the authority which a court has to decide matters that are litigated before it or to take cognizance if matters are presented in a formal way for its opinions. This could be said that it's the power/ authority of the court to decide matters that are brought before him. In this environment, governance over conditioning on the Internet has come a battlefield for the struggle to establish Rule of Law in the Information Society. The rise of the global computer network is destroying the link between geographical position and 1. The power of governments to assert control over online geste; 2. The goods of online geste on individualities or effects; 3. The legality of the sweats of a original autonomous to apply rules applicable to global marvels; and 4. The capability of physical position to give notice of which sets of rules to apply. The net therefore radically subverts a system of rule- making grounded on borders between physical spaces, at least with respect to the claim that cyberspace should naturally be governed by territoriality defined rules. The Internet explosion has generated numerous jurisdictional controversies, putting the onus on courts to determine how to apply major generalities regarding particular governance to the boundary-less world of the Internet. With so numerous outsourcing conditionings in India and the fashionability of networking websites, a fresh continuum of cases related to" particular Victimization" and" profitable Offences" in the nature of data protection, cyber vilification, security, etc. have evolved. Hacking initiated at one place negatively affects any other place institution and brings them to limbo.[15]

Relevant Legislations of Cyber Jurisdiction in Bangladesh:

1) Information & Communication Technology Act, 2006: Section 4 of the ICT Act, 2006 implies that the Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence involves a computer, computer system or computer network located in Bangladesh.[16]

2) The Penal Code, 1860: According to Penal Code, 1860, discipline of offences committed beyond, but which by law may be tried within Bangladesh any person liable, by any Bangladesh Law, to be tried for an offence committed beyond Bangladesh shall be dealt with according to the vittles of this law for any act committed beyond Bangladesh in the same manner as if similar act had been committed within Bangladesh. According to Section 4 of the Penal Code, 1860, Extension of law to extra-territorial offences the vittles of this law apply also to any offence committed by- (i) any citizen of Bangladesh in any place without and beyond Bangladesh; (ii) any person on any boat or aircraft registered in Bangladesh wherever it may be.

3) The Code of Criminal Procedure, 1898: The law provides that indeed if a citizen of Bangladesh outside the country commits the offence, the same is subject to the governance of courts in Bangladesh. In Bangladesh, governance in cyberspace is analogous to governance as that relating to traditional crimes and the conception of private territoriality will prevail. handed, also, that any proceedings taken against any person under this section which would be a bar to posterior proceedings against similar person for the same offence if similar offence had been committed in Bangladesh shall be a bar to further proceedings against him under the Extradition Act, 1974, in respect of the same offence in any home beyond the limits of Bangladesh.[17]

SEVERAL ACTS FOR CYBER SECURITY OF NETIZENS'

Information and Communication Technology Act, 2006: In order to stop cyber-crimes The Information and Communication Technology Act 2006 (ICT Act) was first passed by the government of Bangladesh. In order to give information and communication technology legal status and security, the government established the aforementioned Act. The government has also made multiple amendments to the Act.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

The Digital Security Act, 2018

The ICT Act was superseded by this legislation, which also broadened the list of crimes involving cyber activity. Stricter rules about hate speech, fake news, rumours, and online defamation were implemented under the Digital Security Act. Some have criticized it for perhaps endangering the right to free speech.

A digital security law in Bangladesh is the Digital Security Act, 2018, which was revised as the Cyber Security Act in 2023. The purpose of this act is to stop the dissemination of hate speech, racism, extremism, sectarianism, terrorist propaganda, and hostility towards religious or ethnic minorities via print, electronic, or social media. The government has the authority to impose fines or varying prison sentences for any content found on the internet or in other media that is considered sexual or inappropriate. This is a contentious law, and because of some of its imprecise and vague language, which is vulnerable to interpretation or abuse, there was concern that it would be used to silence critics of the administration. This statute has been applied to cyber criminals, activists, and journalists, leading to lawsuits and arrests. It is referred to as a "Draconian" legislation.[18]

The Copyright Act, 2005

The Copyright (Amendment) Act, 2005 was enacted on May 18, 2005, amending the Copyright Act, 2000, which had superseded the Copyright Ordinance, 1962. This Act states that copyright registration in Bangladesh is optional rather than required. The registration creates proof of ownership in the event that copyright is contested. The Act complies with both the TRIPS Agreement and the Bern Convention. It has many clauses about copyrights for digital media and computer programmes, databases, movie theatre, broadcasting, performers' rights, phonograms, and other things.[19]

Cyber Fraud in Bangladesh

In the modern, convergence of communication era, Online payments, online banking, online shopping, In virtually every area of our lives, including online ticket purchases, internet lotteries, data transfers, data conversations, and auctions, we must traverse a superhighway.

Therefore, we must navigate online. While the ICT Act, 2006 does not define cyber fraud, it does contain certain sections that are pertinent to Bangladesh's efforts to prevent and manage cyber fraud. Any individual who accesses, downloads, copies, or extracts data, computer data base, or information from any computer, computer network, computer system, computer data or data base, or data stored in removable media, such as CDs, Floppy discs, or DVDs, without the owner's permission, or who causes similar damage, faces a minimum sentence of seven years in prison and a maximum sentence of fourteen years in prison, as well as tk one crore in compensation.[20]

Case Study Bangladesh Cyber Heist

In 2016, hackers infiltrated the Bangladesh central bank's computer systems and attempted to steal nearly $1 billion from its account at the Federal Reserve Bank of New York. They used malware to compromise the bank's SWIFT network, which is used for international financial transactions. However, the majority of the transactions were blocked, but $81 million was successfully transferred to accounts in the Philippines.[21]

While the hackers were able to transfer a significant amount of money, a portion of it was eventually recovered. Investigations were conducted by Bangladeshi authorities with assistance from international agencies. In 2019, a court in Bangladesh sentenced eight people to death for their involvement in the cyber heist, including a former bank employee and several IT technicians.[22]

(a) *RAB vs. Rumana Manzur*

Rumana Manzur, a Canadian-Bangladeshi woman, was the victim of a horrific cyber-crime incident in 2011. Her husband, Hasan Sayeed Sumon, brutally attacked her, gouging out her eyes and severely beating her after accusing her of having an affair because of her increased social media activity. Rumana Manzur was a Fulbright scholar and a faculty member at Dhaka University. Her case highlighted the dangers of cyber-bullying and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

domestic violence fueled by suspicions arising from online activities.[23]

Hasan Sayeed Sumon was arrested and charged with attempted murder and torture. In 2013, a court in Bangladesh sentenced him to life imprisonment for his heinous crime against his wife. This case shed light on the intersection of cyber-crime and domestic violence, emphasizing the need for stricter laws and better enforcement to protect individuals from such atrocities.[24]

WANNA CRY RANSOMWARE ATTACK (2017)

In May 2017, a Ransomware assault known as Wanna Cry struck systems running Microsoft Windows. The attack encrypts data and demands payment in Bitcoin. It was a global cyber-attack. Because of a flaw in the Server Message Block (SMB) protocol, the attack gained momentum very quickly. More than 200,000 machines across more than 150 nations were impacted, including FedEx, the National Health Service (NHS) in the UK, and Telefonica, a Spanish telecommunications business.

Before the victims' files could be unlocked, the Ransomware demanded money. In addition to demanding payment in Bitcoin, the attackers threatened to remove the encrypted files if the ransom was not paid in a predetermined amount of time. The assault took advantage of a flaw in previous iterations of Windows, for which Microsoft had patched the system months beforehand. Eventually, the attack was linked to the North Korean cyber-criminal group Lazarus Group, which is well-known for carrying out intricate cyber operations. The event made clear how crucial it is to maintain cyber-security hygiene, update software often, and create data backups in order to lessen the effects of cyber-attacks. It also emphasized the necessity of international cooperation in order to successfully defend vital infrastructure from cyber-attacks.[25]

CHALLENGES OF CYBER LAW

1. Accessing electronic evidence is difficult, and service providers don't cooperate. Even though the legislation has this provision, it is not implemented since many law enforcement officials are unaware of it and their authority to require compliance from service providers.

2. The intricate process of gathering proof in order to win cases and obtain a head start on the internet makes the research necessary. Examples include numerous instances of online attacks against young women. Additionally, there have been documented instances of businesses in competition being harmed by the internet. Finding the information's original source is challenging in this case. considerably within the nation, the Cyber Crime Unit and other law enforcement units frequently cannot access the information source. The situation becomes considerably more complicated when the service provider is not within our jurisdiction, in which case we would need to rely on requests for mutual legal assistance. When information is disseminated over social media sites like Whats App, this frequently occurs.

3. Handling electronic evidence improperly, a few of our investigators are inexperienced in obtaining electronic evidence in accordance with our admissibility guidelines. As a result, the courts dismiss really important evidence.

4. Chain of custody, maintaining appropriate custody is crucial to ensuring the admissibility of electronic evidence in court when it is transferred between different institutions.

5. The digital forensic techniques available to law enforcement institutions are insufficient for gathering electronic evidence. Occasionally, investigators need help with digital forensics, and that means turning to private cyber forensic firms.

6. Lengthy waits related to the collection of evidence. This is typically the situation when dealing with bank frauds enabled by the internet, as attacks on the bank's software originate from outside the nation. Cooperation from foreign nations is required for investigations and prosecutions, and this frequently necessitates a lengthy evidence collection process.[26]
7. Lack of a trend and skilled labour to design and implement the growing problems in cyberspace.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

8. In addition to giving rise to cyber-terrorism and a lack of societal awareness, cyber-attacks have also made cyber-crime hackers more skilled every day due to the abundance of online resources on hacking and cyber-crime.

9. Bangladesh Cyber Cell's computer sector understanding is minimal. The majority of candidates in the cyber cell department lack literacy and understanding compared to the younger hackers in the community.

10. Compared to other crimes in the nation that require attention, the government budget passed for security purposes in cyber law enforcement and training programmes is less. The government is typically unable to identify the original sources of cyber-crime networks and is also unable to apprehend hackers or cyber-terrorists because of the most recent technologies and the youthful, updated cyber-hacker population's faster working speed, which consistently outpaces the government departments and sectors in charge of cyber-crime.

11. The government's existing laws and regulations for the improvement of cyber cells in India are insufficient; more work needs to be done, and stricter laws should be passed for the improvement of cyberspace. Internet users also need to be aware of government programmes and schemes, as they relate to other criminal activities. The improvement of national privacy and our everyday lives both depend on cyber-crime.[27]

12. The present scenarios of cyber laws in Bangladesh are not exhaustive due to the loopholes in different areas. This should be standardizing with global perspectives.

FINDINGS

The major findings of the study are following:

1. The Information and Communication Technology Act of 2006 is insufficient to address cyber-crime.

2. Only a few provisions of the Information and Communication Technology Act of 2006 address cyber-crime, and even then, the details are unclear.

3. According to the Information and Communication Technology Act of 2006, punishment is not suitable for the type of crime that is being sought after.

4. Pornography Act 2012 and Child Pornography also enacted for protect the cyber from the pornography. Cyber-crime will not be covered by this Act in its entirety. This is the procedure; no one posts porn on the internet, but where is the fix?

5. Cyber-crime is not mentioned in our Penal Code; nonetheless, Section 13 lists comparable offences.

6. Just cellular networks are covered by the Bangladesh Telecommunication Act of 2001. It is either not very current or does not address cyber-crime in any way.[28]

RECOMMENDATION

1. If the government of Bangladesh wants to tackle cyber-crime in a comprehensive manner, a separate agency for cyber-crime protection should be created in Bangladesh. This agency will be fully governmental and will be under the Ministry of Home Affairs. The headquarters of the agency will be in the capital Dhaka. The name of the agency is "**Cyber Crime Protection Unit**"(**CCPU**). The head of this agency will be the Director General (DG).

The main functions of this agency will be to ensure the safety of netizens, arrest cyber criminals and bring them under the law, crack down on all cyber related crimes and take appropriate steps to reduce cyber-crimes, along with issuing legal guidelines for public awareness.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

The responsibilities of a "Cyber-crime Protection Unit" typically include investigating cyber-crimes, analyzing digital evidence, tracking cyber-criminals, developing strategies to prevent cyber-attacks, and collaborating with other law enforcement agencies and organizations to improve cyber security systems.

The agency will function somewhat like the "**Rapid Action Battalion or RAB**" organization of the police. This agency will act very quickly wherever cyber-crime takes place. This "Cyber Crime Protection Unit" will have one zone in each division of Bangladesh. Like **CCPU-1**, **CCPU-2**, **CCPU-3**, **CCPU-4**, **CCPU-5**, **CCPU-6**, **CCPU-7**, **CCPU-8**.

Each zone of this agency will have as many sub-zones as there are districts. These sub-zones will tackle all types of cyber related crimes from district level to upazila level and remote areas and the officers of this agency will have powers to arrest cyber criminals, and take further action as per cyber-crime laws.

The person who can arrest cyber criminals under this agency in remote areas will be of the rank of ASI of Police. So if the government creates a government agency called "Cyber Crime Protection Unit" and specific laws to manage this agency, then cyber related crimes can be curbed and this "Cyber Crime Protection Unit" will play an important role in building a "**SMART**" Bangladesh.

2. As soon as possible, fix the defects of the ICT Act 2006, and after the amendment, the Act should be implemented in the whole of Bangladesh.

3. Amending existing laws in the country to strengthen cyber laws, introducing new laws, and creating new enforcement mechanisms to deal with growing cyber threats. The input and consultation of legal experts and policymakers are essential for the development of this new enforcement mechanism.

4. Exemplary and effective punishment of criminals for cyber-crimes is very important so that cyber criminals will not have the courage to commit such crimes later. Then individuals and organizations can be easily protected from online threats. Cooperating with legal authorities is essential to ensuring appropriate consequences for cyber-criminal activity.

5. Ensuring the independence of Cyber Tribunals is essential to maintaining fairness and impartiality in the trial of cyber-related crime cases. According to the jurisdiction of these tribunals as per the cyber law, if the tribunals can conduct trials independently, then it is possible to suppress cyber-crime in Bangladesh.

6. To protect the violations of human rights, cyber laws should be enacted in such as way so that these will not inconsistence with international laws.

7. This law can be developed through the national laws and implementations of various mechanisms.

CONCLUSION

Bangladesh government will be able to crack down on cyber-crime. If the existing cyber laws against cyber-crime in Bangladesh are fully implemented and the weaknesses of the cyber laws are fixed. Besides, if the law enforcement agencies properly cooperate with the government of Bangladesh, there is no doubt that cyber law can play a very important role against cyber-crime. Cyber legislation is crucial to safeguarding netizens' privacy in the modern digital era. Through legislative frameworks and regulations, cyber law establishes boundaries and imposes consequences for privacy infringement. They support the prevention of data breaches, the management of surveillance tactics, and the security of personal data. Cyber law is, in essence, necessary to protect users right to privacy online, foster netizen confidence, and ensure everyone can use the internet safely.

FOOTNOTES

[1] https://www.usegenie.ai/?gad_source=1&gbraid=0AAAAAokY3Pc1EoM_q1pFr1eRSpFwo09Rf, Accessed on 16 January, 2024.

[2] K. Mahmood & M. A. Hossain, "Cyber Laws in Bangladesh: An Analysis of the Information and

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue VIII August 2024

Communication Technology Act, 2006," International Journal of Cyber Security and Digital Forensics 6, Issue 3, 2017, p 66-79.

[3] Ibid.

[4] Universal Declaration of Human Rights, 10 December 1948, Article 19.

[5] https://www.usegenie.ai/?gad_source=1&gbraid=0AAAAAokY3Pc1EoM_q1pFr1eRSpFwo09Rf, Accessed on 1 march, 2024.

[6] Article 19 of the International Covenant on Civil and Political Rights (ICCPR), 1966

[7] Article 19, of the Universal Declaration of Human Rights (UDHR) 1948

[8] Article 19 of the ICCPR

[9] The United Nations Human Rights Council report, January 2012

[10] Article 2 of the Office of the United Nations High Commissioner for Human Rights

[11] Article 39 of the Constitution of the People's Republic of Bangladesh

[12] The International Telecommunication Union (ITU), May 17, 1865.

[13]https://edu.gcfglobal.org/en/useinformationcorrectly/copyright-and-fair-use/1/Accessed on 28 March, 2024.

[14] Article 42 of the Constitution of the People's Republic of Bangladesh

[15] Ibid

[16] Section 4 of the Information & Communication Technology Act, 2006

[17] Section 179, ibid

[18] https://en.m.wikipedia.org/wiki/Digital_Security_Act,_2018, Accessed on 23 april, 2024.

[19] https://www.wipo.int/wipolex/en/legislation/details/11172, Accessed on 28 april, 2024.

[20] Ahmed Dr. Zulfiqar, March 2009, A Text Book on Cyber Law in Bangladesh, Hasan Law Books, Islamia Market, Nilkhet, Dhaka-1205, p 392.

[21] https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery,Accessed on 5 may, 2024.

[22] https://en.prothomalo.com/bangladesh/crime-and-law/x9ljt3o7vd, Accessed on 6 may, 2024.

[23] https://www.tbsnews.net/features/panorama/rumana-monzur-story-domestic-abuse-survivor-legal-pioneer-834281, Accessed on 7 may, 2024.

[24] Ibid

[25] https://www.usegenie.ai/?gad_source=1&gbraid=0AAAAAokY3Pc1EoM_q1pFr1eRSpFwo09Rf, Accessed on 12 may, 2024.

[26] https://rm.coe.int/16806be179, Accessed on 15 may, 2024.

[27] https://www.legalserviceindia.com/legal/article-9458-trending-issues-and-challenges-in-adjudication-of-cyber-crime.html, Accessed on 15 may, 2024.

[28] https://www.academia.edu/41139813/_Prevention_of_Cyber_Crime_in_Bangladesh_Researcher, Accessed on 16 may, 2024.