International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 29-07-2024, Accepted: 28-08-2024, Published: 12-09-2024
Volume 10, Issue 5, 2024, Page No. 31-33

Cyber crime in Bangladesh: Need for unique cyber law

Rajia Sultana
Associate Professor, Department of Law, Rajshahi Science and Technology University, Natore, Bangladesh

Abstract
The topic of rising cybercrime and other technology-related crime in Bangladesh is crucial right now. The recent hacking of the RAB website and email is one example of how cybercrime is becoming a danger to the Bangladeshi government. Because we lack the necessary and appropriate legislation to safeguard such sorts of crime, cybercriminals are essentially free to engage in such criminal activity. The Information and Communication Technology Act was passed by the Bangladeshi government in 2006, and it was updated in 2013 as the ICT (Amendment) Act-2013. This Act contains a number of anti-cybercrime provisions; however, they are not comprehensive or specific enough. There is a possibility to regain safety after committing crimes by enacting this law. A thorough Cybercrime Protection Act ought to be implemented in light of these realities. In order to limit the occurrence of cybercrime, this article seeks to advocate for the adoption of more cybercrime legislation as well as the promotion of those that have already been passed. This essay has a particular impact on the areas of our personal lives, places of employment, bodies that make policy, and thinkers.

Keywords: Cybercrime, technology, criminals, ICT, protection

Introduction
The way we live has undergone significant change as a result of new communication systems and digital technology. The Internet has grown considerably in the last ten years. International borders are no longer a barrier to this type of crime, which takes use of the current state of technology in the world market. The number of internet users in Bangladesh is quickly rising. Although cybercrime is slowly rising in Bangladesh, there is currently no system in place to address it. Cybercrime includes all illegal activities involving networks and computers. It also includes conventional crimes committed online [1]. A increasing number of states have enacted or are considering proposing new legislation on cybercrime-related charges, however as of yet, Bangladesh's government has not made any significant efforts to enact cyberlaw in our nation. The internet has grown to play a significant role in our lives. Bangladesh's information technology industry is expanding. Bangladesh, like any other country, is attempting to keep up with the speed of modern technology, which is why there is a need for particular legislation to manage cybercrimes. The creation of cybercrime legislation is also essential if Bangladesh wants to safeguard its online security.

Definition of cyber crime
Cybercrime can broadly be defined as a criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (theft), and electronic fraud [2]. Anything from downloading pirated music to stealing millions of dollars from online bank accounts falls under this category. Cybercrime also encompasses non-financial violations like developing and disseminating viruses on other computers or publishing private company data online.

Different types of cyber crime
Cybercrimes can be basically divided into 3 major categories:
1. Cybercrimes against persons.
2. Cybercrimes against property.
3. Cybercrimes against government.

Cybercrimes against people can take many different forms, such as sending child pornography or harassing someone over email while using a computer. Crimes against all types of property fall under the second category of cybercrimes. These offenses include the dissemination of dangerous programs and computer vandalism (theft of others' property). Cybercrimes against the government make up the third type of cybercrimes. One specific type of crime in this category is cyber terrorism [3].

Cybercrime in Bangladesh
Evil and virtue coexist in life. The Internet is also. Despite all the good it may accomplish, the internet also has some negative aspects. The information superhighway, however, does not have police officers patrolling it like traditional communities do, leaving it vulnerable to anything from Trojan horses and viruses to cyberstalking, trademark piracy, and cyberterrorism [4]. A few years ago, a group of people in Bangladesh broke into the Rapid-action battalion's website. Most government institutions felt terrified after reading about this tragedy in the media. No one wants to accept it. Following that, the RAB detained some individuals, who are now in custody. Nobody should employ their newly gained computer abilities in such illicit actions as hacking into significant Government or private websites, according to Shahee Mirza, one of the top RAB website hackers. Many experts in Bangladesh who deal with cybercrimes are terrified after hearing his statement.

Although many of the legal aspects of prosecuting cybercrime are covered under the 2006 Information and Communications Technology (ICT) Act, its effective implementation has not occurred since its adoption. According to experts, the absence of legal backing and a lack of social and public awareness of computer crimes are the key causes of the law's inefficiency. Despite not being prohibited anywhere in the globe, pornography is one of the most common computer crimes in Bangladesh, according to cybercrime analysts. There is already proof that there are localized, illegally hosted pornographic websites [5]. Teenagers in Bangladesh are increasingly adopting cyber cafes as their dating venues today. Newspaper reports claim that a variety of antisocial actions are carried out at these cafes under the pretense of internet browsing. There are separate cabins for couples where they can browse the internet while their private moments are discreetly recorded on film. Later, these images are made accessible online. A person found guilty of posting vulgar or obscene content to a website is subject to a 10-year prison sentence as well as a Tk 1 crore fine, per section 57 of the ICT Act of 2006. However, no one is concerned because there is still no functional cyber tribunal in our nation to handle this issue. Because of this, it is very simple for cybercriminals in Bangladesh to avoid prosecution.

Legal smell regarding cyber-crime in Bangladesh:

On October 8, 2006, the Information and Communication Technology (ICT) Act of 2006 went into effect. In accordance with the 2006 ICT Act, the maximum penalty is 10 years in prison, a fine of up to 10 million Taka, or a combination of the two. The ICT Act 2006 was recently modified by our Parliament, increasing the penalties for cybercrimes to a minimum of 7 years in prison and a maximum of 14 years in prison, a fine of Tk 1 core, or both. The bill invoked section 54 of the Code of Criminal Procedure to enable law enforcement to detain anyone suspected of breaking the law without a warrant by making violations of sections 54, 56, 57, and 61 of the ICT Act, 2006 cognizable and non-bailable. The ICT Act of 2006 did not recognize any of these offenses. All parties involved recognize that the police have abused their authority, nevertheless. Undoubtedly, Bangladesh's ICT Act, 2006, as revised in 2013, is a wonderful achievement in the area of cyber law. Critics point out that the aforementioned Act still has the following specific limitations.

1. Different intellectual property rights, such as copy rights, trade-mark rights, and patent rights of e-information and data, are not addressed by the Act.
2. The law's implementation has a significant impact on Bangladesh's m- and e-commerce [6].

However, it states that the "Information and Communication Technology Act, 2006 and Information and Communication Technology (Amendment) Act, 2013 identify specific offenses that are not covered by the Penal Code. Therefore, it can be claimed that the Penal Code of 1860 does not adequately address cybercrimes. The Information and Communication Technology Act, 2006 was passed by the Bangladeshi parliament and it lists specific actions as crimes [7]. Cybercrimes for Bangladeshi territory are any actions made illegal under the Information and Technology Act of 2006.

Bangladesh plans for strict cybercrime laws

It is important to adopt special laws and create a special tribunal that solely deals with cyber-related issues in order to curb cybercrime. In light of the South Asian nation's explosive growth in information and communications technology and telecommunications networks, Bangladesh is preparing strict measures to combat cybercrime. The ICT sector in Bangladesh has been growing rapidly and is having a significant impact on both the public and private sectors. According to industry estimates, there are currently more than five million personal computers in use in the nation with three million internet users. According to the Joint Secretary to the ICT Ministry, “We have taken steps to facilitate fair and secure use of information technology as the country lacks a complete law to deal with cybercrime.” To address new types of criminality, the government, which has committed to creating a "Digital Bangladesh" by the year 2021, had authorized in principle amending previous legislation that called for lengthy prison sentences and significant financial fines. The administration would engage with the Supreme Court before establishing one or more Cyber Tribunals to ensure the swift and efficient prosecution of the offenses.

Recommendations

The purpose of my research is to recommend that our government pass a cybercrime law so that cybercriminals cannot commit crimes in Bangladesh. My recommendation to the government is to set up a digital forensic lab in our nation for the purpose of looking into and identifying cybercrime. Most of the top private banks in our nation have already launched internet banking as of right now. Based on the Internet and a computer, this online banking. Therefore, it is the responsibility of the government to secure all banks. Terrorists attacked Mumbai in 2008. In that attack, more than 200 people lost their lives. According to the news, terrorists utilize numerous fictitious email addresses in addition to a few fictitious websites to get in touch with their commanders. Close-circuit cameras have revealed that a few terrorists are carrying their own laptops. However, the Mumbai police were unable to stop it since they lacked the knowledge essential to identify it. They completely disregard it, which makes it much simpler for the terrorist to strike their objective [8]. Bangladesh experienced the same kind of attack a few years ago. From 2004 to 2006, J MB killed a great number of people in Bangladesh. The newest technologies were also utilized [9]. Nowadays, terrorists employ cutting-edge technology to perpetrate crimes, making it difficult for law enforcement to catch them until and until they also have access to such technology. For this reason, I recommend that our government set up a digital forensics’ lab in our nation for the purpose of identifying and investigating cybercrime. The creation of cybercrime legislation is also essential if Bangladesh wants to safeguard its online security. A cyber police force is also required to identify online criminals. There are many internet experts available in Bangladesh today who are quite knowledgeable about the internet and the cyber world. Therefore, enacting a cyber law in our country is not difficult. The government only needs to want to carry out this action. Since last year, Bangladesh has been working to combat cybercrime by creating software, educating a group of professionals, and more. Additionally, there is a need for more national training programs, legislation, and enforcement capacity building projects.

Conclusion

Over a billion people are reportedly using the internet in the early years of the twenty-first century. Consumers, businesses, and governments from all around the world must continue to develop strategies to safeguard sensitive personal and commercial data and identify those who plan to use technology for illegal purposes, whether they are based domestically or abroad. The majority of poor nations, including Bangladesh, have limited access to information and the available access is expensive due to inadequate infrastructure and a lack of suitable education. The difficulties are brought on by the absence of an integrated computer security system and of computer security education. As a result, there is a need for cooperation, collaboration, and investment in security, which also helps to establish a culture of security.

References

1. Yatindra Singh. Cyber Laws, 3rd ed. (New Delhi: Universal Law Publishing Co. Pvt, 2007.
2. [http://www.cybercrimelaw.net/Cybercrimelaw.html].
3. Mr. Pavan Duggal. 'Causes of Cyber', International Journal of Computer Science and Information Security, 2009, 3(1).
4. Md. Shah Alam. 'A New Challenge For Law Enforcers', American Journal of Public Health,2004:94(6):951-957.
5. Ripon Kumar Biswas. 'Cyber crimes need more attention', Tuesday, 2008.
6. The Information Technology Act 2006.
7. The Penal Code of Bangladesh 1860.
8. The Times of India, [http://publications.mcgill.ca/reporter/2008/12/page/2/].
9. The Bangladesh Observer (6September2008), [http://www.bangladeshobserver.com/].