



Cyber Property Rights, Its Present Status and Challenges: Bangladesh Context

Kudrat-E-Khuda (Babu)

Associate Professor, Department of Law, Daffodil International University, Dhaka, Bangladesh.

(Corresponding author: Kudrat-E-Khuda (Babu))

(Received 06 January 2020, Revised 02 March 2020, Accepted 03 March 2020)

(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cyber property relates to internet-based property, owned by any person or any organization, which covers all the data people share to the internet. The ICT industry of Bangladesh is expanding quickly and Bangladeshi people are getting in touch with modern communication system. Currently, more than 17 million personal computers are in use here and the number of active internet users is about 10 cores who are connected to different social media and many of them visit different types of websites regularly. The rate of cyber property rights in Bangladesh is increasing but most of the Bangladeshi people have no idea about their cyber property rights which they are sharing on different websites and social media platforms. Even most of them don't know about the negative impacts of data misuse through the internet. At the same time, here many people are using technology to commit crimes. The existing cyber laws of Bangladesh are not adequate to protect cyber property rights and these laws do not cover all the elements of the cyber property. This paper aims to determine how cyber property rights are being violated from website and different types of social media platforms; to determine the effects of violation of those rights in Bangladesh and to find out the mechanisms of cyber property rights protection providing necessary recommendations. Both analytical and empirical research methods have been resorted to complete this study. Primary and secondary sources of data have been taken into consideration for this purpose. The references have been adopted from national and international statutes, books, articles, research reports, acts, newspapers and websites.

Keywords: Bangladesh, Cyber Property, Cyber Property Rights, Cybercrimes, Cyber Law, The Digital Security Act, The ICT Act, Intellectual Property Law, Social Media, Website.

I. INTRODUCTION

Like other developing countries' ICT industry, that of Bangladesh has been expanding quickly and is making its presence wide and strongly felt both in private and public sectors. More than 17 million personal computers are now being used in the country by three million internet users, as ICT industry estimates. Currently, the number of active internet users in Bangladesh is about 10 cores. Among them about 1.8 million are connected to the network, 8.47 crore are connected with mobile internet and 5.733 million with fixed broadband Internet. The huge number of internet users in Bangladesh is connected to the internet and most of them are connected to the different social media and visit different websites also on a regular basis. In the present years, Bangladesh has become one of the most vulnerable countries in cyberspace. Cyber-attacks often take place here causing severe loss of assets. With the increasing number of internet users, the number of attack ratio is also going up [1]. For the protection and control of cyber-crime has to follow the developed country regulation related to cybercrime as well as cyber property rights protection law. Around ten billion Taka in transactions takes place on E-Commerce sites per year according to a 2018 e-Cab report [2]. Social media is widely used in Bangladesh and Facebook is the most popular and usable of different social media platforms with more than 29 million users in the country. Facebook is used to connect to the consumers and is also a major e-Commerce platform in Bangladesh. There are over 8,000 e-commerce Facebook pages in Bangladesh, where many pages are small businesses

using solely Facebook to advertise and sell their products, ranging from clothes, beauty products to food [3]. With faster internet connections, Google cache servers, and better streaming, YouTube is also popular for video watching and sharing in Bangladesh. Everyday lots of people in Bangladesh visit different websites for many reasons and using different social media platforms i.e. Facebook, Twitter, YouTube, etc. they share their data. But most of them do not know properly how to use the internet and share data on the internet. They also don't know whether their data is protected or not in the different platforms of the internet.

II. CONCEPT OF CYBER PROPERTY AND CYBER PROPERTY RIGHTS

Cyber property is a property which is on the cyberspace or internet owned by any person or any organizations. Cyber property covers all the data, which is owned by different people, shared on the internet, like any type of text, photo, video, music, software, etc. There are some of the areas of cyber property covered by intellectual property but not all of them. There are so many areas such as Microblogging, social media post, comments to the social media by users, etc. that intellectual property law does not cover. Intellectual property covers copyright by some of the areas but not all of them of cyber property. Many cyber property rights are being violated every day but those are not covered by intellectual property or any other law in Bangladesh. Cyber property is a new term in Bangladesh which is not used by anyone before. Cyber Property includes all of the property which is on the internet or cyberspace. Over the cyber property, many rights arise in the

different circumstances in the side of the original cyber property owner [4]. Intellectual Property covers some of the components of the cyber property and may give legal remedies but does not covers all of the cyber property components. For the protection and giving legal remedies have to identify all of the cyber property and related rights of cyber property.

The word 'cyber' or 'cyberspace' is connected to computers and the internet. This is a virtual world made by millions of computer connections. The cyber-world, or cyberspace, is more than just the internet [5]. There are two types of the world that have existed in this time. One is the real world and another is the cyber world or cyberspace. Cyberspace is a virtual world created by links between computers, internet-enabled devices, web servers, websites, different types of social media platforms, and other components of the internet's infrastructure. As opposed to the internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state [6]. People share, transfer or show their photos, different types of writing work, intellectual property such as copyright-related work, trademark or trade sign, etc. to cyberspace. It refers to an online environment where many computer users are involved in social interactions and can affect and influence each other. People interact in cyberspace by sharing their data through the use of the website or digital media platforms, such as social networking sites Facebook, Twitter, and Instagram, etc. People share millions of data every day on the internet.

III. REVIEW OF LITERATURE

'Cyber Property Rights' is a very new concept in Bangladesh context. No Bangladeshi writers yet write any book on the cyber property rights. There are very few numbers of books available on cyber law in the local market but no book found on cyber property rights in Bangladesh or on the protection of cyber property rights. But there are some others book related to the present research's objects found in the Internet and different law journals.

The book *Guide to cyber law* by Justice Yasiandra Singh introduces about the cyber world along with the controlling laws for cyber world only. There are 309 pages in this book where nine chapters explore all about the cyber world controlling laws. Another book *Intellectual Property law* by P. Narayan discusses on different type of intellectual property and their rights. The book is relevant to the existing research topic. There are 268 pages where five chapters discuss about the intellectual property, rights and laws.

Cyber Law in Bangladesh by Dr. Zulfiqar Ahmed simply introduces the laws related to the cyber-crimes and crimes using computer and internet. Three chapters of this book discuss recent scenarios of cyber-crime in Bangladesh perspective along with the weakness of laws to prevent cyber-crime in Bangladesh.

The book *Principles of Cyber Law* written by Professor Md. Borhan Uddin where the author discusses different type of intellectual property and there rights. This is co relevant of the current research topic. There are 268

pages in this book where five chapters discuss all about intellectual property, rights and laws.

For preparing the present paper, the author reads many articles and journals i.e. the author reads the article titled *Cyber Property Insurance needs more attention* by Sha Alam Sipon and *New challenge for law enforcers* by Alam. Md. Shah very carefully. Sipon focuses the idea about cyber property and rights related cyber property in his article. In another article by Najrul Islam where the author says about the variability condition about internet privacy and data sharing privacy of Bangladesh. The author of the current paper derive different important information from different web sites also.

The author collects the statement from the persons who are experts in internet and the author uses the several public libraries for several times to collect the data and information to conduct the research. But unfortunately there the author does not find out any book on Cyber Property or Cyber Property Rights. That is why it became difficult for the author to get information on cyber property or protection of cyber property rights.

The author studies the *Information and Communication Technology Act 2006*, the *Digital Security Act 2018* and also reads the *Intellectual Property Law* related to Bangladesh context but does not find any important information there about exact meaning of cyber property or cyber property rights and failure to finds out the punishment for violating the cyber property rights. As a result, the author visits many websites and reads many newspapers and collects the necessary information on Cyber Property Rights and also collects information on protection and control of cyber property rights.

IV. MAJOR DEFINITIONS

A. Website

Website is a digital web presence that enables content such as texts, images, and videos to be displayed on the internet or cyberspace [7]. A website is a collection of publicly accessible, interlinked web pages that share a single domain address name. A website is also known as a web presence [8]. Different types of websites can be found i.e. some websites contain some texts with images and some contain video, PDF file or music for download. These are the entire website in different category i.e. news website, video sharing website, social media website, blog website, music download website, etc. A website may be created for individual data sharing or business purposes. This can be created and maintained by an individual, group, business or organization to serve a variety of purposes. Together, all publicly accessible websites constitute the World Wide Web (WWW).

B. Social media platform

Social media platform is a part of the cyber world which is a web and ISO-based technology providing data sharing, video streaming, photo sharing, chatting, and micro-blogging option to people. Social media platform also provides the ability to create social connectivity and services with complete social media network functionality [9]. Social media platform is a term which is a combination of social media website and different social media apps or software, which provides different options to their users for sharing their data like text,

image, videos, microblog (post of Facebook or small writing). Social Media Platform includes different types of social media websites, apps, and software where some of them are photo-sharing apps or websites, some are video sharing apps or websites and some are social networking websites. All of these websites, apps or software creates a platform named social media platform. Different type of social media platforms are:

- Social networking (Facebook, Google+, LinkedIn).
- Microblogging (Twitter, Tumblr).
- Photo sharing (Instagram, Snapchat, Pinterest).
- Video sharing (YouTube, Facebook Live, Periscope, Vimeo).

C. Cyber property

As mentioned earlier, cyber property means property which is in the cyberspace. Any type of data (text, image, video, music) on the internet and owned by any person or any company or organization and for the misuse of that cyber data is depreciated the owner of that data is called the cyber property. Cyber property is all those properties that are on the internet shared by the people and give permission to access publicly. This is an intangible property by the legal definition of property. Intangible property refers to personal property that cannot be moved, touched or felt, but instead represents something of value such as internet data, negotiable instruments, securities, service (economics), and intangible assets including choice in action. Cyber property may not be physical as we usually define it, but there's no doubt it can be damaged and losses can result [10]. Many times we've all seen that type of property may be corrupted and be misused in different ways from the internet. Few examples of cyber property are Photo, video, news article, blog or microblog (social media post), etc.

D. Cyber property rights

Any cyber property which is on the cyberspace which is owed by any persons or organizations and misused that property by the others people get hampered to the main owner of that data or property [11]. Here a right grows up over that data of the main owner, which may vary to the circumstance this rights is called cyber property rights. Any news article with cover image which is posted to the news website by a news agency is owned by that news agency. If any person without permission copies the published news and cover image and use it at another place, it may cause damage to the news agency who is the main owner. Here the news agency's rights is violated which are related to the cyber property. That's why this right is called cyber property rights.

V. WEBSITE AND CYBER PROPERTY RIGHTS

A website involves a variety of media (text, sound, graphics, databases, etc.), and is thus covered by several different areas of the cyber property and intellectual property law [12]. Website is also known as a web presence [13]. Different types of website can be found i.e. some websites contain some text with images and some contain video, PDF file or music for downloading. These are the entire website in different category i.e. news website, video sharing website, social media website, blog website, music download

website, etc. A website may be created for individual data sharing or business purposes. This can be created and maintained by an individual, group, business or organization to serve a variety of purposes. There are different types of websites such as (a) News website, (b) Blog webpage, (c) E-Commerce website, (d) Video sharing website, (e) Corporate website—which is created by any company or organization for sharing information, (f) Social Networking website and, (g) Job Circular publishing website. All of the categories of the website may contain different types of texts (news, article, blog, information, etc.), Images (website logo, news website cover image, any personal image which is shared by the people), video, etc. These are all the properties of the owner of the website or the organization. Any breach of the data, shared by a person or any organization to a particular website he owns, gets damaged to the original data. The data shared on the website is also called cyber property because it is connected to the internet or the cyber world. The original owner of this cyber property which is on the website has the rights over that data. Any damage or misuse of the data can get legal remedy of the original data owner.

Intellectual property and cyber property correlates them. One is a part of the others. Intellectual property is some of the divisions of property that includes intangible property or creations of the human intellect. Intellectual property law includes some types of intellectual property, and some countries recognize more than others [14]. The most well-known Intellectual property types are copyrights, patents, trademarks, and trade secrets.

Copyrights are covered by copyright ranges from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings. Patent covers an exclusive right granted for a new invention. Generally speaking, a patent provides the original patent creator with the right to decide how or whether the invention can be used by other people whereas a trademark covers a sign or logo which is capable of distinguishing any of the services or goods from other enterprises. Trade secrets are another part of the intellectual property which is IP rights on confidential information that may be sold or licensed. This is all about intellectual property. Cyber property is a part of intellectual property.

VI. THE INFORMATION TECHNOLOGY AND INTELLECTUAL PROPERTY LAW IN THE CONTEXT OF CYBER PROPERTY LAW AND THE IMPACTS OF THESE LAWS ON TECHNOLOGICAL INNOVATIONS

Currently there are two types of worlds. One is the real or natural world and another one is cyber world or cyber space. Cyberspace is a virtual world created by links between computers, internet-enabled devices, web server, websites, different type of social media platform, and other components of the internet's infrastructure. As opposed to the internet itself, however, cyberspace is the place produced by these links. It exists, in the perspective of some, apart from any particular nation-state. People shares, transfers or shows photos, different types of writing works, intellectual property like copyright related works, trademarks or trade sign etc. to

the cyberspace Intellectual property and cyber property have the correlation between them. One is a part of the others. Intellectual property is a division of property that includes intangible property or creations of the human intellect. Different types of intellectual properties are included among the subject matters of intellectual property law and some countries recognize more than others [15]. The most well-known intellectual property types are: copyrights, patents, trademarks, and trade secrets. Copyrights is covered by copyright range from books, music, paintings, sculpture and films, to computer programs, databases, advertisements, maps and technical drawings. And the patent covers an exclusive right granted for a new invention. A patent provides the original patent creator with the right to decide how or whether the invention can be used by other peoples. Where trademark is covered sign or logo which is capable of distinguishing any of the service or goods from other enterprises. Trade secrets are another part of the intellectual property which is IP rights on confidential information which may be sold or licensed. This is all about intellectual property and the cyber property is a part of the intellectual property.

Cyber property is a property which is on the cyberspace or internet owned by any person or any organizations. Cyber property cover all the data which is owned different people shared to the internet like any type of texts, photo, video, music, software etc. There is some of area of cyber property covered by the intellectual property but not all of them. There are so many areas do not cover intellectual property law such as Microblogging, social media post, comments to the social media by users etc. Intellectual property covered copyright by some of area but not all of them of cyber property. Many of cyber property rights violated every day but which is not covered by intellectual property or any others law in Bangladesh.

The cyber security policy is a developing mission that caters to the entire field of Information and Communication Technology (ICT) users and providers. It includes –

- Home users
- Small, medium, and large Enterprises
- Government and non-government entities

It serves as an authority framework that defines and guides the activities associated with the security of cyberspace. It allows all sectors and organizations in designing suitable cyber security policies to meet their requirements. The policy provides an outline to effectively protect information, information systems and networks. It gives an understanding into the Government's approach and strategy for security of cyber space in the country. It also sketches some pointers to allow collaborative working across the public and private sectors to safeguard information and information systems. Therefore, the aim of this policy is to create a cyber security framework, which leads to detailed actions and programs to increase the security carriage of cyberspace.

Technological innovation may be classified in several ways: product vs. process, radical (basic or fundamental) vs. incremental (improvement), and disruptive vs. sustaining (sequential and/or

complementary). Other important types of (non-technological) innovations that do not result from scientific and/or technological R&D, but are often crucial for profitably marketing the products and services resulting from the investment made in R&D are: marketing innovation, institutional innovation, and complementary innovation [16].

As there are many players involved in facilitating the market success of an innovation, the effective use of the tools of IP will play an important role in reducing risk for the players involved, who may then be able to reap acceptable returns for their participation in the process [17]. IP plays an important role in facilitating the process of taking innovative technology to the market place. At the same time, IP plays a major role in enhancing competitiveness of technology-based enterprises, whether such enterprises are commercializing new or improved products or providing service on the basis of a new or improved technology. For most technology-based enterprises, a successful invention results in a more efficient way of doing things or in a new commercially viable product. The improved profitability of the enterprise is the outcome of added value that underpins a bigger stream of revenue or higher productivity.

Technology innovation has accelerated progress in Information and Communications Technology (ICT), especially in the mobile phones sector. Concurrently, local, national, and international governments are enforcing stricter regulations to protect natural resources and human health. In the past few decades there has been a revolution in computing and communications, and all indications are that technological progress and use of information technology will continue. The revolution in information and communication technology has changed not only our lives but also the way how people do business. Using information technology, companies possess the potential to reach more customers, introduce new products and services quickly, and collaborate with suppliers and business partners from all over the world. Transformation from industrial society to information society and industrial economy to knowledge economy is a result of the impact of ICT and Internet use [18].

VII. CYBER PROPERTY RIGHTS IN BANGLADESH

A huge number of internet users in Bangladesh are connected to the internet and most of them every day connect themselves to the different social media and many visits to some websites. 'Cyber Property Rights in Bangladesh'- along with its sub-points discusses the present scenario of Bangladeshi social media users and that of other platforms where people share their data which is breached in different ways every day. In recent years, Bangladesh has become one of the most vulnerable countries in cyberspace. Cyber-attacks often take place, which causes loss of assets. With the increasing number of internet users, the number of attacks ratio is also going up. For the protection and control of cyber-crime, the developed country's regulations related to cyber-crime as well as cyber property rights protection law should be followed.

VIII. PRESENT SCENARIO OF BANGLADESH

The e-Commerce Association of Bangladesh (e-Cab) and the trade body for e-Commerce in Bangladesh conducted a survey and estimated that there are 3 lakh blog websites in Bangladesh where people share their writing, 7000 thousand plus online news portals sharing news online, 700 e-Commerce sites and around 8,000 e-Commerce pages on Facebook. Facebook remains a popular method for advertising and selling products, to a point that many businesses forgo creating websites. Around 10 billion takas in transactions take place on E-Commerce sites per year according to a 2018 e-Cab report [19]. Social media is widely used in Bangladesh and it is the most popular and usable of different social media platforms with more than 29 million users in the country. Facebook is used to connect to the consumers and is also a major e-Commerce platform in Bangladesh. There are over 8,000 e-commerce Facebook pages in Bangladesh, where many pages are small businesses using solely Facebook to advertise

and sell their products, ranging from clothes, beauty products to food [20]. With faster internet connections, Google cache servers, and better streaming, YouTube is also popular for video watching and sharing in Bangladesh. Every day a lot of people in Bangladesh visit different websites for many reasons and using different social media platforms i.e. Facebook, Twitter, YouTube, etc. share their data. But, most of them do not know properly how to use the internet. They do not also know how to share data on the internet. They also don't know whether their data is protected or not in the different platforms of the internet.

A. Common vulnerabilities in cyber space of Bangladesh

In recent years, Bangladesh has become one of the most vulnerable countries in cyberspace. Cyber-attacks often take place, causing loss of assets. With the increasing number of internet users, the number of attacks ratio is also going up [21].

Table 1: Encounter rate and CCM in Bangladesh compared to world.

Metric	2015	2016	2018	2019
Encounter rate, Bangladesh	44.10%	39.70%	42.50%	57.20%
Worldwide encounter rate	17.60%	15.30%	17.80%	20.80%
CCM, Bangladesh	29.8	32.7	25	40.3
Worldwide CCM	5.4	8.4	6.1	16.9

In recent times, the statics of cyber-crime has mostly grown up by using the computer and the internet. Here the primary target is data (maybe photo, texts, video, music or any component related to the internet or website). We have also seen the massive violation of copyright and trademark in the social media platforms as well as websites. Any person may use another person's data, which is shared on the internet, and may commit any crime to the internet or social media platform by the misuse of the shared data. In the years 2018 to 2019, there are around 679 people arrested by the Criminal Investigation Department (CID) for committing different crimes using social media platforms. The perpetrators, mostly, blackmail people using their photos or video they share on the internet easily because there is no protection of cyber data or cyber property rights. In recent times, a domain name was created similar to the Bangladeshi leading newspaper prothomalo.com. In different ways, people breach cyber property and also commit crime by using this property every day in Bangladesh.

B. Legal fabric of Bangladesh regarding cyber property rights

There are some laws in Bangladesh relating to the cyber property or the cyber-crime protection and prevention of crime. Some of the laws have few provisions which are connected to the cyber-crime and the protection of cyber property rights. The main laws relating to cyber property in Bangladesh are:

- The Information and Communication Technology Act, 2006 (The ICT Acts, 2006)
- The Digital Security Act, 2018
- The Penal Code, 1860.

The Penal Code of Bangladesh has very few provisions regarding cyber squatting. But in case of cyber-crime or

violation of cyber property rights like copyright, without permissions of the owner and using their cyber property at another place, or any crime committed by the use of the cyber property- there is nothing contained in our penal code. That's why it can be said that it is not easy for our government to control violation of cyber property rights by using some provision of the Penal Code.

The ICT Act, 2006 passed by the Government of Bangladesh (Later, the Bangladesh Parliament amended the ICT Act on 6 October 2013) is the most recent statute enacted by the government of Bangladesh to consolidate Computer related matters and prosecute computer and computer network related offence. This statute contains several provisions regarding damage to computer and computer systems. Most of the provisions do not cover all about the cyber property and protection of cyber property rights. The Section 66 of the ICT Act provides Punishment for interfering with computer source documents. Section 66 says only about the few matters related to hacking or interferes with others' computers without permissions [22]. All of the ICT Act has been made for the protection of hacking or preventing the offense of "hacking". This does not cover the cyber property in social media platforms and websites.

Another law related to cyber property in Bangladesh is the Digital Security Act, 2018. This Act is enacted to ensure National Digital Security and enact laws regarding Digital Crime Identification, Prevention, Suppression, Trial and other related matters [23]. Some of the provisions of this Act cover some elements of the cyber property or cyber property rights protection but not all. It is not possible to cover all the things by implementing just only one act. In order to control cyber

Property Rights we need to have one specific cyber law in our country.

C. Weakness of cyber laws in Bangladesh

In Bangladesh, there have few laws relating to cyber-crime which do not cover all of the contents of Cyber property [24]. The offences of the Bangladesh Information and Communication Technology Act, 2006 are non-cognizable offence in nature under section 76 subsection 2. As per the section, the victim has to file an allegation to the law enforcement agencies to get remedy. This is the main weakness of the said act [25]. At the time of enactment of the said Act, it was said in section 68 that a special tribunal would be the named Cyber Tribunal and would be established in every district of Bangladesh. But the matter is yet to be materialized as only a single tribunal has been established in Dhaka City, not in every district. The main weakness of the cyber laws of Bangladesh are:

- Most of the cyber laws are passed by legislation without sufficient public debate, which do not really serve the desired purpose.
- Ambiguity in the definitions – Most of the laws in Bangladesh make the entire essential clause in complex word; People do not understand or catch them.
- Not cover all areas- The cyber law of Bangladesh does not cover all the cyber property or components which may cause damage to any person.
- There is no cyber law in Bangladesh that is uniform in nature.
- One important reason is that cyber laws are not achieving complete success is the lack of awareness among the people about their rights.
- Jurisdiction issues are other loopholes of Bangladeshi cyber laws.
- Time limitation- In Chapter 8 of the ICT Act creates a cyber tribunal to adjudicate cybercrimes where judges of the tribunal have to complete the judgment procedure within 6 months of filing the case. This is another limitation of cyber laws in Bangladesh.

D. Cyber property rights in developed countries

Cyber Property Rights protection and control is the primary matter in all of the developed country, i.e. USA, Australia, Switzerland, England, etc. Different countries have enacted their national cyber laws keeping in mind their own national requirements. The United States cyber security laws and privacy system are most powerful for the protection and control of the cyber-crime and violations of cyber property rights. The State's' privacy system relies more on post hoc government enforcement and private litigation [26]. Currently, cyber security regulation comprises of directives from the Executive Branch and legislation from Congress that safeguards information technology and computer systems. In August 2012, the Australian Government passed the Cybercrime Legislation Amendment Act 2012 (CLAA) for the protection and control of cyber-crime [27]. The purpose of the CLAA was to enable Australia to protect and control cyber property-related crime as well as prevent the violation of cyber property rights in Australia. The neighboring country of Bangladesh is India which has updated cyber

laws for prevention and control of cyber-crime and protection of cyber property rights. The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce [28]. Most of the developed countries make cyber laws for protection and control of cyber-crime as well as cyber property rights on cyberspace. We should follow the cyber law framework of the developed country and make updated cyber law for preventing cyber-crime and protecting cyber property rights. In the USA where Google has to pay millions of dollar for taking their users' information but in Bangladesh there is no particle example like that. Here people may use the cyber property for crime in cyberspace easily and this trend is rising quickly [29]. For making better and securing cyberspace for Bangladeshi people has to make updated rules and regulation and execute that for prevention of cyber property rights violation and protection of cyber property rights in Bangladesh.

IX. IMPACTS FOR VIOLATION OF CYBER PROPERTY RIGHTS

The impact of the violation or infringement of Cyber Property Rights covers both Civil and Criminal areas. An individual or a company or organization is the original owner of the data he/she share on the internet. When any person, illegally or without permission of the original owner, copies the shared data from the internet and uses it for another area for commercial purpose or any criminal act, it raises civil or criminal impact. Cyber Property is multi-disciplinary, covering criminal and civil issues ranging from financial crimes to criminal acts [30].

A. Economical impact for violation of cyber property rights

Cyber Property is multi-disciplinary, covering criminal and civil issues. Violation of cyber property rights by any misuse of cyber property or any other act relating to against original cyber property owners may consist of civil or economic impact. That means an infringement of cyber property rights formed some of the economic impacts.

B. Cause of damage

Any violation of cyber property rights may cause huge damage to both the victim and the person who is related to this work. Sometime violation may be one of the causes for decrees the company's trust or reputation which is also a civil nature impact. If a person willingly or unwillingly takes any attempt that is related to the cyber property (copy logo of a company, domain squatting, stealing information, unauthorized use of any data), he may cause a huge economical loss of any individual or any company. On November 28, 2018, Rapid Action Battalion (RAB) claimed to have arrested two people for their involvement in creating a website similar to Bangladeshi leading newspaper online version prothomalo.com and identical to those of different local media outlets and circulating false and "anti-government" news through them [31]. Prothomalo.com is an original and authorized website of the *Prothom Alo*

newspaper. Around five million visitors visit the online version of the *Prothom Alo* newspaper. Income generates by visiting the website through the ads of this website. For creating a similar website of prothomalo.com, many users bounce and visit the fake and similar website of *Prothom Alo*. Consequently, *Prothom Alo* faced a huge economic loss as well as a negative impact to its users as the fake website published false news and anti-government news. Here *Prothom Alo* faced an economic loss for the misuse by their name and there data. Here *Prothom Alo*'s cyber property rights have been violated.

C. Loss of reputations

Misuse of the cyber property may cause damage to reputations of any individual or any company or organization. When a person collects some information from any social media platform or any website (Facebook profile or Facebook page or any other social media platform or any website) and then creates a duplicate page, profile or website as the same of the real name of any individual or any company or organization, he publishes some fake news or any news or information that goes against the person or company or share anti-government news or intimidating someone by using the fake name of Facebook page or website. This kind of work damages a person or the company's reputation. This is another economic impact of violations of cyber property rights. So, it can be said that the violations of cyber property rights may cause losses of any individual or company's reputation.

D. Infringement of cyber property rights and criminal impact

The infringement of cyber property may constitute a criminal impact because the cyber property is a multi-disciplinary subject which covers both criminal and civil issues. By the misuse of cyber property or violation of cyber property can arise criminal liability of any person who is actively connected to this issue [32].

E. Harassment

Over the world, social media websites such as Facebook, Twitter, and LinkedIn, as well as photo-sharing platforms like Instagram, video sharing platforms like Youtube, Vimeo, etc. make information about private individuals more readily accessible than ever. Unfortunately, this accessibility sometimes facilitates cyberstalking, harassment, or cyberbullying and cybercrimes using those of cyber data or cyber property. Many times we have seen some people being victims of harassment from social media platforms. A person may create a fake account by using another individual's photo or name or information from a website or social media and continuously harasses the person in different circumstances of harassment [33]. Even, the perpetrators share false information or share nude photos in the fake account or profile they create taking the real name or image or information of another person from the social media platforms such as Facebook, Twitter, etc. These fake profiles are opened for various reasons:

- Harassing a group or an individual
- Hiding actual identity for doing illegal works on Facebook

- Spreading anti-religious, anti-national sentiment
- Business purpose
- Spamming
- Political propaganda

Suicide Attempts due to Cyber Crimes and Harassment in Bangladesh (Source: Bangladesh Woman Lawyers' Association, 2014). This figure shows that the amount of suicide attempts due to cyber harassment is increasing every year. Many of today's psychiatrists are concerned about the rise of cybercrime [34]. This crime can be a great threat to the mental health of today's youth and teenagers as well as other age groups.

Table 2. Suicide Attempts Due To Cyber harassment in Bangladesh.

Year	Suicide Attempts
2015	28
2016	31
2017	39
2018	48

F. Spreading false news and rumor about someone

When news is published or broadcasted in mainstream media, the news is checked, edited and verified by an editor. And he is responsible for the news to the law enforcement agency.



G. Misuse of picture

Screenshot has been collected from Kick Off group helpline where a friend of the victim is seeking help to stop spreading rumor [35]. Sometimes, the victim's photo is edited with a nude background. Those photos spread online quickly. People with lower minds watch those photos and made bad comments. And this type of harassment brings a lot of mental and social problems to the victim.

H. Online piracy

Online piracy is another element for infringement of cyber property owner rights. By unauthorized copy or download of a picture, any piece of writing, video or information of any company or organization by any person and then using that data in another place or selling or using it for commercial purposes will be online piracy. Online piracy violates the original owner's rights which may call a violation of cyber property rights. This may consist of civil and criminal impact.

I. Legal consequences of cyber property rights violations

Cyber property rights violations prescribe harsh penalties for cyber property theft. In most cases, cyber property misuse or theft and infringement violations are charged as criminal issue [36]. They can result in consequences such as:

- Criminal fines

- Imprisonment for several years, depending on the nature of the charges
- Seizure of the property which is used for violation of cyber property rights
- Loss or suspension of a business operating license
- Civil charges filed by the victim of the crime (for instance, for lost business profits)

This is the legal consequence of cyber property rights violations which is not proper or adequate for that issue. If we want to prevent the violation of the cyber property rights on online sphere, we need to modernize the cyber laws of Bangladesh as well as that of Police and BTRC. Without placing proper people in the proper position, we can't solve the misuse of cyber property and protect cyber property rights from the Internet.

The impact of cyber property rights violations is wide and prejudicial for both the victim and the perpetrator. It can be so pungent when its impact will be deep. Due to the violation of cyber property rights, a victim may suffer huge economical or reputational losses. The person, who commits crimes using cyber property or by misusing cyber property, must be punished by law. If we want to prevent the violation of the cyber property rights on online sphere, we need to modernize the cyber laws of Bangladesh as well as Police and BTRC. Without placing proper people in the proper position, we can't remove misuse of cyber property and we did not protect cyber property rights from the Internet [37]. We have to create awareness about the impact of infringement of cyber property or property rights among people. Some of the initiatives need to be taken to make the people aware of their cyber property sharing and rights. People have to be made aware of how to get a remedy when their cyber property rights are violated. They also have to be informed about the preventive measure for the protection of cyber property rights in cyberspace.

X. CYBER PROPERTY RIGHTS IN BANGLADESH: PROTECTION AND CONTROL

With the rapid growth of information and communication technology (ICT) and with the spread of the internet, people get the touch of modern communication systems such as social media platform websites, etc. But at the same time, many people commit crime by using this technology. By the use of social media or websites, anyone can violate or commit digital crime easily [38]. The impact of cyber property rights violations is very wide and prejudicial for both the victim and the perpetrator. It can be too pungent when its impact will be deep. Due to the violation of cyber property rights, a victim may suffer huge economical losses or reputational losses. It is high time we should take some initiatives for the protection and control of violation of such crime as well as protect the cyber property rights of the people.

A. Governments initiative for protection and control of cyber property rights violation

For the protection of cyber property rights and control of violation of cyber property rights in Bangladesh, the Government must take initiatives to overcome this issue. The government of Bangladesh has already taken some measures to prevent cybercrime and cyber data protection. It has adopted a cyber-security

declaration 2017 asking the organizations to develop modern and actionable cyber security road maps to be approved and monitored by the top management [39]. Our Government makes special cyber security experts and representatives of local and foreign technologists, cyber security giants and protects people's cyber property rights in Bangladesh.

The Governments also have taken some other initiatives for the protection of cyber property rights in Bangladesh, such as:

- Make adequate rules and regulations for the control of all Social Media Platforms and data protection
 - Give proper training to the people about cyber data protection
 - Make a well-trained law enforcement agency to overcome this issue.
 - Make a modern cyber tribunal for tried all of the cases
- The Government of Bangladesh has some infrastructures for preventing and protecting of cybercrime. However, Bangladesh attributes considerable importance to the protection of critical information infrastructure. Therefore, the Government will lead the cyberspace security and cyber data privacy protection of cyber property rights to the people. The Government's procurement process will mandate the inclusion of security clauses in service contracts to encourage the development of secure cyberspace technologies. Besides, the following recommendations may be taken into consideration by the Bangladesh Government to protect cyber property rights in Bangladesh.
- To make regulation for the control of social media data sharing or data management in Bangladesh.
 - To make adequate cyber laws in Bangladesh that covers all elements of the cyber property.
 - To establish one digital forensic laboratory in Bangladesh for investigation and detection of cyber-criminal.
 - To follow General Data Protection Regulation (GDPR) in Bangladesh for data privacy.
 - To make regulation for website and web server for the protection of cyber property rights.
 - To make public awareness about cyber-crime and impact of cyber property rights violation, as well as of how they can protect their cyber data.
 - To make a special cyber security team for monitoring the cyber property.
 - To implement existing cyber laws and intellectual property laws.
 - To develop cyber-crime related legislation in Bangladesh.
 - To stop online information piracy by implementing regulations.
 - To establish cyber tribunal in every district in Bangladesh for giving remedies to people who are the victim of cyber property rights violations as well as cyber-crime.

It is not possible for the person alone to prevent and protect cyber property rights violations and cyber-crime in Bangladesh. The sluggish reality is Bangladesh Police or BTRC doesn't have the technological ability to prevent or track down cybercriminals as well as to

prevent cyber property rights violations from the Internet [40]. The government of Bangladesh and all the people of Bangladesh who use the internet and social media also have some responsibility. The government alone cannot prevent violations of cyber property rights if we do not help the government to do this. We have to aware of the impact of cybercrime as well as our cyber data violation.

XI. RECOMMENDATIONS

Cyber property is all those properties that are on the internet shared by the people and give permission to access publicly. In simple words, any data, owned by someone, which is on the internet and anyone may access it, is called cyber property. Over this property, the owner has the rights and anyone will not violate that rights. Every day people share a huge amount of data on the internet i.e. website or any other social media platform. Some people knowingly or intentionally commit cyber-crime or violate other cyber property rights by using this property. The impact of these acts is a huge economical loss or arise criminal liability to the people. So, this is high time to take some measures or initiatives for the protection of crime using cyber property and control of those crimes. The following initiatives can be taken by the government and concerned authorities along with the people to protect of crime using cyber property and control of those crimes.

A. To make adequate Rules and Regulations

For the protection of cyber property rights in Bangladesh, adequate rules and regulations should be taken or implemented. Because in Bangladesh existing laws related to cyber-crime are not adequate for the protection of cyber property rights. The existing laws related to cyber security and cyber-crime do not cover all the elements of the cyber property. The present laws include some of the elements of cyber property and give inadequate remedies to the victim.

- The Information Communication Technology Act 2006
- Digital Security Act 2018
- The Penal Code 1860

These are the existing laws for preventing cyber-crime and cyber security in Bangladesh. But the main problem is that all of the existing laws are not adequate for the protection of cyber property rights in all the areas. Some of the cyber property does not include any laws of Bangladesh such as Microblogging, Facebook status, photo from social media, Comment of the social media, any texts which represent any individual or any company or organizations, etc. All of the micro cyber property sometimes causes economic or reputational losses or criminal liability for misusing or committing a crime by that cyber property. That's why it is high time for creating adequate laws and regulations for the protection of cyber property rights and the prevention of its violations in Bangladesh. We have to enact more laws relating to cyber property and amend the existing laws for including the entire element of cyber property in Bangladesh. This initiative can reduce violations of cyber property rights in Bangladesh.

B. To Raise Awareness

A comprehensive and sustained initiative is raising public awareness of the risk and impact of the violation of cyber property rights and. The explosion of connected devices -- from smart refrigerators, lighting systems, heating and air conditioning, security services to autonomous automobiles -- puts an exclamation point behind the importance of cyber property rights protection for individual users and organizations of all sizes and levels of internet users of Bangladesh.

Awareness should cover:

- Impact of violations of cyber property rights
 - How to use social media platforms properly and secure personal data.
 - How to protect one's cyber property rights by the help of laws
 - Awareness about rules and regulation related to cyber property
- This type of public awareness may help to prevent and protect cyber property rights violations in Bangladesh.

C. To Make Rules for Cyber Property Management

Initiatives should be taken for generating data sharing rules and regulations for Bangladeshi social media and internet users. The government may generate rules and implement those for cyber property/cyber data management in Bangladesh. Developed countries have implemented the data share and management rules for the protection and prevention of cyber property rights violations form cyberspace. We should also create rules now to prevent cyber property rights violations and make a safe cyber environment for Bangladeshi people.

D. To Effect Executives Actions

The executive authority will be essential to contribute to the protection of cyber property rights in Bangladesh territory. The police force and other law enforcement agencies can contribute a lot to the cyber property rights violation as well as control of cyber crime. They can trace the offender who breaches another person's cyber data rights and takes away to the court to execute them by laws. The executive authority also can agree to the different social media platforms and websites as well as web-hosting providers for the protection of a person's cyber data in Bangladesh. Law enforcement agencies and BTRC are still ineffective. Because of their ineffectiveness, the criminal gets extra privileges to violate other cyber property rights.

E. To Implement the EU General Data Protection Regulation (GDPR) in Bangladesh

The General Data Protection Regulation-GDPR is a regulation in European Union law for data protection and privacy of all individuals within the jurisdiction of the European Union. GDPR is the largest European regulation of personal cyber data protection over the last 20 years and will affect almost every international and national organization. Why is GDPR important for a Bangladeshi? In short, the answer is, GDPR is a local law with global reach. The provisions of the General Data Protection Regulation are applicable to all data processing activities related to personal data of EU individuals, including offering goods and services to the EU and monitoring their behavior.

If GDPR framework is followed in our country, cyber data protection will be more efficient with the global cyber data protection style. According to article 4, GDPR data is to be protected as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This also includes IP addresses and content data such as comments on blog articles. All of the cyber data is protected by this European Union regulation. When it directly applies in our country or when create laws following the GDPR framework, we can protect our cyber data privacy and prevent cyber property rights violations.

XII. CONCLUSION

Bangladesh has a huge number of internet users and day by day it is increasing continuously. There are a lot of internet users using different types of social media and visiting different types of websites for connecting other people or acquire information every day. In this process of communication to other, people share their valuable data on the internet. But the problem is their cyber data is not protected on cyberspace. For the inadequate laws and lack of knowledge about the impact of cyber data, many times on different grounds people suffer huge economic loss, reputation loss, harassment; blackmailing and any other different criminal issues arise. Here someone easily misuses another person's cyber data by collecting that from the internet. Over the world, most of the developing countries like Bangladesh have limitations in access to information and the available access is not affordable because of the inadequacy of the existing laws and regulations with implementing the body as well as the non-availability of appropriate cyber awareness. The challenges are posed by the lack of an integrated computer security system and education about cyber security and protect their cyber property from others. These are the existing laws for preventing cybercrime and cyber security in Bangladesh. But the main thing is all of the existing laws are not adequate for the protection of cyber property rights in all the areas. All of the micro cyber property sometimes causes losses of economic damage or reputational losses or may cause criminal liability. That's why it is high time for making adequate laws and regulations for the protection of cyber property rights violations in Bangladesh. The sluggish reality is Bangladesh Police or BTRC doesn't have the technological ability to prevent or track down cybercriminals as well as to prevent cyber property rights violations from the Internet. The governments of Bangladesh and all the people who use the internet and social media also have some responsibility to protect own cyber property rights. The more public awareness about the value of their property and impact on the violations of cyber property can help to overcome this issue in Bangladesh. If the government makes adequate laws which cover all their elements of cyber property

and protection and control of cyber property rights violation properly, it will be very easy to overcome this issue in Bangladesh and make a safe cyber environment for Bangladeshi internet users.

ACKNOWLEDGEMENTS

The author would like to express his gratitude to his student Md. Mynul Islam and his younger brother Md. Sujon Ali for their kind efforts to conduct this study.

REFERENCES

- [1]. Hossain, T. (2019). Common Vulnerabilities in Cyber Space of Bangladesh Common malware families encountered in Bangladesh. *Bangladesh Information and Security Journal*, 1(1), 11-23.
- [2]. Firoz, A. (2016). Present Internet Users and Websites in Bangladesh. *The Daily Star*, p.5.
- [3]. Khan, A. (2015). Social Media Users in Bangladesh. *The Daily Star*, p.9.
- [4]. Nationwide®. (2003). Cyber Property Insurance: Prose and Corns. Retrieved from: <https://www.nationwide.com/what-is-cyber-insurance.jsp>
- [5]. Ahmed, Z. (2009). A Textbook on Cyber Law in Bangladesh. Dhaka: National Law Book Company.
- [6]. Akhtaruzzaman, M. (2012). Freedom of the Press in South Asia. Dhaka: Dhaka International University Press.
- [7]. Alam, M. S. (2007). Cyber-crime: a new challenge for law enforcers. *Journal of University of Information Technology & Sciences*, 2(1), 25–37.
- [8]. Pal, A. (2019). Rise in cybercrime worries women. *The Dhaka Tribune*, p.7.
- [9]. Buono, F. M., & Friedman, J.A. (2000). Maximizing the enforceability of click wrap agreements. *Journal of Technology Law & Policy*, 4(3), 20-32.
- [10]. Bleyder, K. (2012). Cyber Security: The Emerging Threat Landscape. Dhaka: Bangladesh Institute of Peace and Security Studies.
- [11]. Beck, U. (2002). The terrorist threat: world risk society revisited. *Theory, Culture & Society*, 19: 39–55.
- [12]. Ehsanul, K. (2017). Media and Cyber Laws in Bangladesh. Dhaka: Sufi Prokashoni.
- [13]. Firoz, A. (2016). Present Internet Users and Websites in Bangladesh. *The Daily Star*, p.10.
- [14]. Gbenga, B. (2004). Information communications technology and e-commerce: challenges and opportunities. *The Journal of Information, Law and Technology*, 1(2), 121–122.
- [15]. Gandhi, K. (2012). An Overview Study on Cyber-crimes in Internet. *Journal of Information Engineering and Applications*, 2(1), 1-6.
- [16]. David, R., Geoffrey, R., & Robert, B. (2000). Collaboration and the Successful Use of Information and Communications Technologies in Teaching and Learning Geography in Higher Education. *Journal of Geography in Higher Education*, 24(2), 263-270.
- [17]. Boldrin, M., & Levine, D. (2002). The Case against Intellectual Property. *The American Economic Review*, Vol. 92(2), 209-212.
- [18]. Berisha, A. (2015). Impact of Information Technology and Internet in Businesses. *Academic Journal of Business, Administration, Law and Social Sciences*, 1(1), 73-79.

- [19]. Halder, D., & Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. USA: Hershey.
- [20]. Faruk, A. (2016). Present Internet Users and Websites in Bangladesh. *The Daily Star*, p. 11.
- [21]. Ariful, K. (2015). Social Media Users in Bangladesh. *The Daily Star*, p. 10.
- [22]. *ibid.* (2019).
- [23]. Shanaj, M. (2018). ICT laws which work. *The Dhaka Tribune*, Retrieved from: <https://www.dhakatribune.com/opinion/2018/09/02/ict-laws-which-work>.
- [24]. The Digital Security Act. (2018). Available: <https://www.cirt.gov.bd/wp-content/uploads/2018/12/Digital-Security-Act-2018-English-version.pdf>
- [25]. Habib, M. (2015). The limitations of ICT and Cyber Security Acts. *The Daily Star*, p.8.
- [26] Essays, UK. (2018). Weakness of Cyber Law in Bangladesh Information Technology Essay. Retrieved from <https://www.ukessays.com/essays/information-technology/weakness-of-cyber-law-in-bangladesh-information-technology-essay.php?vref=1>.
- [27]. Hasson, A. (2018). Understanding the United States Cyber Security Laws and Regulation (literally) [Blog Post]. Retrieved from <https://www.appknox.com/blog/united-states-cyber-security-laws>
- [28]. Hoque, G. (1992). *Mass Media Laws and Regulations in Bangladesh*. Singapore: Asian Mass Communication Research and Information Centre.
- [29]. Jaspreet, S. (2015). Violence against women in cyber world: A special reference to India. *International Journal of Advanced Research in Management and Social Sciences*, 4(1), 60-76.
- [30]. Pal, A. (2019). Rise in cybercrime worries women. *The Dhaka Tribune*, p. 10.
- [31]. *ibid.* (2016).
- [32]. Khan, J. (2018, November 30). 2 arrested over fake news sites. *The Daily Star*, p.3.
- [33]. Halder, D., & Jaishankar, K. (2011). *Cybercrime and the Victimization of Women: Laws, Rights, and Regulations*. USA: Hershey.
- [34]. Maruf, A., Islam, R., & Ahamed, B. (2010). Emerging cyber threats in Bangladesh: in quest of effective legal remedies. *The Northern University Journal of Law*, 1(1), 112–124.
- [35]. Pavan, D. (2014). Causes of Cyber Crimes. *International Journal of Computer Science and Information Security*, 3(1), 586-590.
- [36]. Paranjape, V. (2008). *Criminology and Penology*. Allahabad: Central Law Publications.
- [37]. Tikk, E. (2011). Ten Rules for Cyber Security. *Survival: global politics and strategy*, 53(3), 119-132.
- [38]. Altaf, H. (2011). *Laws of Intellectual Property*. Dhaka: Bangladesh Law Book Company.
- [39]. Borhan, U., & Kader, M. (2014). *Oporad Biggan porichity*. Dhaka: Kamrul Book House.
- [40]. Azad, M., Mazid, N., & Sharmin, S. (2017). Cyber Crime Problem Areas, Legal Areas and the Cyber Crime Law. *International Journal of New Technology and Research*, 3(5), 1-6.

How to cite this article: Kudrat-E-Khuda (2020). Cyber Property Rights, its Present Status and Challenges: Bangladesh Context. *International Journal on Emerging Technologies*, 11(2): 735–745.