

## **Right to Privacy in Cyberspace: The Case of Bangladesh**

**Joysree Das**

Student of LL.B. (Hons) State University of Bangladesh

**Md. Mahafuzur Rahman**

Student of LL.M. State University of Bangladesh

### **Introduction**

Right to privacy is a broad area which demands to be overlooked carefully. It is such an idea which varies from country to country based on its religion, culture, social structure and customs as well. In almost all the international instruments the rights to privacy is given priority. Privacy is protected under the Universal Declaration of Human Rights 1948, the International Covenant in Civil and Political Rights 1966 and in many other intentional and regional human rights treaties. Both national and international instruments gives right to privacy an importance place.

### **Defining Right to Privacy:**

Privacy is the most cherished freedoms in a democratic country.<sup>1</sup> Privacy, an interest of the human personality, protects the inviolate personality, the individual's independence, dignity and integrity.<sup>2</sup> Generally, the phrase "right to privacy" is used to mean that each individual has the right to choose whether he wants to share information about his or her private life, habits, acts and relations with others. But it is not an easy task to have an authoritative definition of the concept 'privacy'.

### **Privacy as Fundamental Right:**

The constitution of Bangladesh in article 43 expressly declares that every citizen shall have the right to the privacy of his correspondence and other means of communication. A creative interpretation of article 32 of the constitution may also implicit the idea of right to privacy in the fundamental right to life and liberty. This proposition was extended by Mr. Justice Subba Rao<sup>3</sup> where he contended that- the concept of liberty under the constitution was comprehensive enough to include privacy on a person's house, where he lives with his family and that nothing is more deleterious to a man's physical happiness and health than calculated interference with his privacy.

### **Privacy and Free Expression:**

Privacy and freedom of expression is two distinctive ideas from the perspective that where the right to privacy is insisted on, the freedom of expression is made limited, i.e., where the freedom of expression is ended the right to privacy is activated. Innovations in some technologies have facilitated increased possibilities for communication, and protections of free expression and opinion, enabling anonymity, rapid information sharing, and cross-cultural dialogues. At the same time, changes in technologies have given rise to increased opportunities for State surveillance and intervention into individuals' private communications.

### **How Privacy is threatened: Abuse of Process:**

#### ***The Digital Security Act***

The Act is problematic in many ways. It is believed by the many that the Act will hurt the freedom of expression with its problematic nature. There are lots of chances to abuse the process of this law. Most talked are of its three sections.

---

<sup>1</sup> US SC Justice Louis Brandeis ,quoted in warren, Samuel and Brandeis, Louis;"The Right to Privacy",4(1890),Harvaed Law Review;pp 193-220.

<sup>2</sup> Bloustein, Edward," privacy as an aspect of Human Dignity" ,39(1964),New York University Law Review ,at p.971.

<sup>3</sup> Kharak Singh v. State of U.P (AIR 1963)

First of all section 21 says anyone who spreads negative propaganda against the Liberation War or the Father of the Nation, using digital devices, or instigates such acts will risk being sentenced up to 14 years' jail or a fine of up to Tk 1 crore or both. He or she will face up to life imprisonment or Tk 3 crore fine or both for committing the offence for the second time, it said. Section 25 on the other hand says that a person may face up to three years in jail or Tk 3 lakh fine or both if he or she is found to have deliberately published or broadcasted in a website or electronic form -- something which is attacking or intimidating or which can make someone dishonest or disgruntled; if he or she knowingly publishes or broadcasts false and distorted (full or partial) information to annoy or humiliate someone, or to tarnish the image of the state or to spread rumor.

A person will face up to five years in jail or Tk 10 Lakh or both for committing the offence for second time, it is said. Thus section 28 says a person may face up to seven years in jail or Tk 10 lakh fine or both if he or she is found to have deliberately published or broadcasted something in a website or in electronic form or get it done to hurt one's religious sentiment and values. A person will face up to ten years in jail or Tk 20 lakh or both for committing the offence for the second time as stated in the act. In addition, section 32 says a person may face up to 14 years in jail or Tk 20 lakh fine or both on the charge of spying if he or she illegally enters the offices of government, semi-government and autonomous bodies to gather information and uses electronic device to record something secretly.

If that person commits the crime again, he or she will face life imprisonment or a maximum fine of Tk 1 crore or both Information and Communication Technology Act: The Act was mainly blamed for its section 57 where it gave scope of arbitrary use of power and hurt the freedom of expression in cyberspace. However it is alleged that the section 57 of the ICT Act has returned in the garb of section 32 of Digital Security Act. Many criticized the matter, saying the government had just modified the ICT Act's Section 57 and people will still lose freedom of expression because of the new law.

### **Right to Privacy in International Instruments**

Right to privacy has been given the status of human rights under different human right instruments. The International Covenant on Civil and Political Rights (ICCPR), the UN Convention on Migrant Workers<sup>4</sup> and the UN Convention on Protection of the Child<sup>5</sup> adopt the same language<sup>6</sup>. Another remarkable effort should be mentioned; The Convention on Cybercrime (ETS-185) also known as Budapest Convention in 2001. This Convention criminalized certain action or omission and tried to bring the countries under one umbrella to solve various existing challenges. A more common but non-binding guideline is there named UNCITRAL Model Law on Electronic Commerce (1996) that is aimed at setting a universal structure to protect economic rights rather grievous human rights issues<sup>7</sup>.

### **Right to Privacy in Bangladeshi Laws**

Despite the fact that there is no particular legislation for protection in cyberspace, however some safeguards can be formulated with respect to protecting privacy of an individual considering some existing laws of Bangladesh. They are the available laws to prevent cyber crimes against women in Bangladesh and its problems are given below-

Information and Communications Technology (ICT) Act 2006 (amended in 2013):

Section 57 of the ICT Act states that anyone can be penalized for "any false and obscene posts online" for a maximum of 10 years and maximum fine of 1 crore. However, it does not define what constitutes "obscene".

Cyber Pornography can be tried under section 57 of the said Act.

<sup>4</sup> A/RES/45/158 25 February 1991, Article 14.

<sup>5</sup> UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.

<sup>6</sup> International Covenant on Civil and Political Rights, <<http://www.hrweb.org/legal/cpr.html>>, accessed on 8 November 2018

<sup>7</sup> universal-individual-privacy-human-rights-cyberspace , retrieved from:<https://lawhelpbd.com/cyber-law/universal-individual-privacy-human-rights-cyberspace>, accessed on 10 November 2018

The judges and the lawyers are the experts of laws, not of technology, more specifically of internet technology. So judges as well as the lawyers should be trained and made expert in technological knowledge for ensuring the justice of technological disputes.

Operation and Monitoring Department of BTRC: Bangladesh Telecommunication Regulation Commission (BTRC) has the authority to monitor hateful content, such as death threats and derogatory comments targeted against particular communities. However, they don't seem to be focusing on these issues, argues Sara. "Of course, the question then arises: what do you prioritize more, the immediate death threats against bloggers, for instance, or the general hate speech on social media? The problem is that our regulators don't seem to be doing either."

Cyber Wing of Bangladesh Police: Bangladesh police have opened a cyber wing to deal with the increasing number of cyber threats and it is responsible for monitoring cybercrimes and tracking the criminals. Police is going to form a "cyber cop" division to tackle the looming social dangers of cybercrime<sup>8</sup>. But gender-based violence on online is not covered as a specific action.

### **Courts Dealing With Cyber Crime**

#### ***Cyber Tribunal***

Under section 68(1) of the Information and Communication Technology Act, 2006 (hereinafter referred to as the Act) the Government of Bangladesh is empowered to establish one or more Cyber Tribunal (hereinafter referred to as CT). The Tribunal shall comprise with- A Session Judge, or Additional Session Judge.

All offences under the Act shall be tried by the Cyber Tribunal. The Tribunal will not try any other offence as per section 68(3) of the Act.

- The Tribunal will be established by an official gazette.
- The Tribunal will follow the Code of Criminal Procedure so far as practicable.
- The Tribunal will complete a trial within six months of framing charge.

#### ***Cyber Appellate Tribunal***

Section 82 of the Act empowers the government to establish one or more Cyber Appellate Tribunals (hereinafter referred to as CAT).

- The CAT will entertain appeal from CT.
- It will consist of a chairman and two members to be appointed by the Government.
- Chairman: who is or was a judge of the Supreme Court or eligible to be appointed a judge of the Supreme Court.
- Members: One member is District Judge or a retired District Judge. Another member is a person having knowledge and experience in information and communication technology.
- The Chairman and the members will be appointed for a minimum of three years to a maximum term of five years period and the terms and condition of their service will be fixed by the Government.
- The decision of the CAT is final.

### **Necessity to Secure Cyberspace**

From that point of view, some cyber analysts have indicated that in a tight race, cyber actors do not need to create major disruption. In this context, a few of them are suggesting that hackings leading to affecting the voting process in votings but in some precincts do not use verifiable paper audit trails to confirm results, this could directly affect results<sup>9</sup>.

---

<sup>8</sup> cyber-cops-to-fight-online-crime , Retrieved from<<https://www.dhakatribune.com/uncategorized/2014/04/20/cyber-cops-to-fight-online-crime>>, accessed on 9,November,2018

<sup>9</sup> need-stop-misuse-cyberspace, Retrieved from: <https://www.dhakatribune.com/uncategorized/2016/11/06/need-stop-misuse-cyberspace>, accessed on 25 August , 2018

For example, when we talk about our election, particularly National Parliamentary Election, we talk about the vulnerability of the Electronic Voting Machine. So cyber privacy is interconnected even with our right to vote.

Furthering “national interest priorities” through the use of cyberspace is not new. Many countries over the years have used this as a weapon to further their own agenda. It would be useful at this point to recall some of them. In very recent time Bangladesh Government has given a proposal to the *facebook*, a popular social media network, to require NID and cell phone number to open account to prevent misuse of cyberspace and ensure national security<sup>10</sup>.

### **Conclusion**

It is important for everyone to understand that attacks against the computer system may be carried out in different ways. Graham Day in his book namely “*Security in the Digital World*”, says: “Attackers are slowly discovering all the ways to make devices to be used to attack others. As this knowledge develops, the number and sophistication of attacks also increase<sup>11</sup>.” Therefore to ensure the cyberspace to be secured it is an urgent need to update the provisions and punishment within the existing laws and make new laws keeping pace with the changed situation and use of technologies in Bangladesh.

---

<sup>10</sup> ফেসবুক-খুলতে-এনআইডি-যাচাইয়ের-প্রস্তাব, Retrived from  
<https://www.prothomalo.com/technology/article/1559015/ফেসবুক-খুলতে-এনআইডি-যাচাইয়ের-প্রস্তাব>, accessed on 19 November,2018

<sup>11</sup>why-is-cyber-crime-increasing, retrieved from: <https://www.itgovernance.co.uk/blog/why-is-cyber-crime-increasing/>, accessed on 20 November, 2018