Cyber law and its weakness: Bangladesh perspective

MD.MEHEDI HASAN
THIRD YEAR
ROLL: 09029015
DEPT.OF LAW & JUSTICE
RAJSHAHI UNIVERSITY

The world over cyber crime has taken deep root and the use of cyberspace by sophisticated cyber criminals has assumed serious proportion today. Criminals and terrorists associated with drug trafficking, terrorist outfits are employing Internet for anti social, anti national and criminal activities with impunity.Terrorist groups are deftly using Internet for passing on information with regard to executing various terrorist acts having serious negative impact on human life. The cyber-terrorists have even acquired the capability to enter computer systems using"logic bombs" (coded devices that can be remotely detonated), electro magnetic pulses and high-emission radio frequency guns, which blow a devastating electronic wind through a computer system. The hackers have gone to the extent of distributing free hacking software — *Rootki*t, for instance — to enable an intruder to get root access to a network and then control as though they were the system's administrators.Many instances of cyber crime involve techno-trespass and unauthorized access to the computer system and data or programmes stored in computers. This access could be without authorization or exceeding the authorization given to an individual. The un authorized access may lead to theft, alteration or destruction of data, tampering with computer programmes or other software, damage to computers or computer systems including damage to data stored on storage devices, such as hard disks,floppy disks, CD-ROMs, etc. This would, in turn, lead to serious financial loss to theorganisation. Thus computer crime today has emerged as a challenge for criminaljustice system and law enforcement.Studies have shown that computer criminals are generally computer professionals or computer-literate persons and are not history sheeters and mostly without previous criminal record. Studies also show that the threat is mostly from employees or from those with access to the system, such as maintenance personnel, hardware and software vendors, etc. however, external threats via remote access have shown an increasing trend.

Cybercrime and Scenario in Bangladesh:

In 2008 a petty hacker of Bangladesh named Shahi Mirza hacked the RAB's website. Moreover he confessed to police that not only RAB's website but also other national govt. and non govt. and international site had been hacked by him for a long time. Totally he hacked 21 website together with Army's website. So it is clear to us that the cyberspace of Bangladesh is

not secured.

Today the cyber criminals enter into the computer system or network with their talents, sufficient and special higher knowledge and technique neglecting legal process. That is why they cause great harm or loss to individuals and state by theft of important and private information by selling that information by theft of bank accounts money by transferring civil information to the opponent party. There are some laws regarding this but the cyber crime is not controlled. Recently the Bangladesh ICT Act-2006 has added to the list. Its some sections was amended in 2009 where as the highest punishment is 10 years imprisonment or find up to 1 crore. Though this Act is not sufficient to prevent the cyber crime. Then everyday should have knowledge about that act and penalty. On the otherhand the govt and concerned authority should continuously amend this law. Because some harm derived from cyber crims is beyond the crore money which encourage the cyber criminals.

To define and amend certain parts of law relating to legal recognition and security of information and communication technology and related matters the Information and Communication Technology Act- 2006 was enacted.According to the ICT Act the cybercrime shall be treated as non cognigible offence that is why the police can't arrest the criminals without warrent except some cases.

Chapter eight section 54 to 67 of the ICT Act 2006 describe the cybercrimes both civil and criminal matters. The followings shall be treated as crime;

- Unauthorized copying, extracting and downloading of any data, database
- Introduction of virus
- Damage and disruption to computer system and computer network
- Denial of access to authorized person to computer
- Providing assistance to make possible to commit to crime
- Hacking with computer system
- Tampering computer source documents
- Electronic forger for the purpose of cheating and harming reputation
- Using a forged Electronic record
- Publication of digital signature certificate for the fraudulent purpose
- Confiscation of computer, network etc
- Publication of information which is obscene in electronic form
- Misrepresentation and suppressing material facts for obtaining digital signature certificate
- Breachof confidentiality and privacy
- Publishing false digital signature certificate

If any person does any crime under section 54 of the ICT Act 2006 he will be given penalty of maximum 10 years rigorous imprisonment or fined up to 10 lacs taka or for the both of above.

If any person does any crime under section 55 he will be given penalty of maximum 3years imprisonment or fined up to 3 lacs taka or with both. Whoever commits hacking under this act shall be punished of maximum 3 years imprisonment or fined up to 1 crore taka or with both. Whoever commits such crime

under section 57 of this act shall be punished of maximum 10 years imprisonment or fined up to 1 crore taka or with both. Penalty for failure to surrender license is 6 month imprisonment or fined up to 10 thousand taka or with both. Penalty for failure to comply with order made by the controller is maximum 1 years imprisonment or fined up to 1 lacs taka or with both.Penaly for violation of the order of the controller in emergency period is maximum 5 years or fined up to 5 lacs or with both.Punishment for unauthorized access to protected system is the maximum 10 years or fined up to 10 lacs or with both. Penalty for false representation and hiding information is maximum 2 years imprisonment or fined up to 2 lacs or with both.Penaly for discloser of confidentiality and privacy is

maximum 2 years imprisonment or fined up to 2 lacs or with both.Punishment for publishing false digital signature certificate is maximum 2 years imprisonment or fined up to 2 lacs or with both. Penalty for Publication of digital signature certificate for the fraudulent purpose is maximum 2 years imprisonment or fined up to 2 lacs or with both.

Analysis of the statutory provisions: ** Weakness of ICT ACT

The Information Technology Act 2006 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

1.* The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose** * *_*

Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and

it is also a fact that sufficient time was not given for public debate.

2. *"Cyberlaws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime*" –

Mr. Pavan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the I.T.Act 2006 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime.

At this point I would like to express my respectful dissent with Mr. Duggal. I feel that the above statement by Mr. Duggal is not fundamentally correct. The reason being that the preamble does state that the Act aims at legalising e-commerce. However it does not stop here. It further amends the I.P.C., Evidence Act, Banker's Book Evidence and RBI Act also. The Act also aims to deal with all matters connected therewith or incidental thereto. It is a cardinal rule of interpretation that "*text should be read as a whole to gather the meaning". It seems that the above statement has been made in total disregard of this rule of interpretation. * The preamble, if read as a whole, makes it very clear that the Act equally aims at legalising e-commerce and to curb any offences arising there from.

3.*Cyber torts-* NO mention of cybere torture

The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T.Act 2006 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T.Act 2006 read with the Penal Code is capable of dealing with these felonies.

4.*Cyber crime in the Act is neither comprehensive nor exhaustive*-

Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- "The IT Act, 2006 is not comprehensive enough and doesn't even define the term 'cyber crime"*.** * Mr. Duggal has further commented, "India, as a nation, has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day

in the form of new kinds of crimes*."** *

I feel that a new legislation on cyber crime is totally unwarranted. The reason is that the new legislation not come alone but will bring with it the same confusion, the same dissatisfaction and the same desire to supplant it by further new legislation. Mr. Duggal has stated above the need to supplement IPC by a new legislation. If that is the issue then the present legislation along with the Penal Code when read harmoniously and co- jointly is sufficient to deal with the present problems of cyber crime. Further there are other legislations to deal with the intellectual property crimes on the cyber space such as the Patents Act, Copy Right Act, Trade Marks Act.

5.*Ambiguity in the definitions-* Definitions are not specific.

The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The *infamous * * go2nextjob** * has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the netizens are till s. 66 exists in its present form.

Further section 67 is also vague to certain extent. It is difficult to define the term *lascivious information or obscene pornographic informa tion. * Further our inability to deal with the cases of cyber pornography has been proved by *the Bal Bharati case*.* *

6. *Uniform law*- * * Not uniforem between nations

Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

7.*Lack of awareness-*

One important reason that the Act of 2006 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling *Microsoft pirated software*over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for *online cheating *by buying Sony products using a *stolen credit* * card*.* 7*

8*. Jurisdiction issues*-

Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2006 is very silent on these issues.

9. *Extra territorial application-*

Though S.4 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

10. *Raising a cyber army-*

By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the*Cyber Crime Investigation Cell (CCIC of the Central Bureau of Investigation (CBI 11 *is definitely a welcome step in this direction. There are man cases in which the C.B.I has achieved success. The present position of cases of cyber crime* 7* is –

Case 1: When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

Status: Probe on

Case 2: CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.

Status: Chargesheet not filed

Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

Status: Pak not cooperating.

11. *Cyber savvy bench-*

Cyber savvy judges are the need of the day. Judiciary plays a vital role in

shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the *P.I.L., which the Kerela High Court* has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. *Mr T.K.Vishwanathan*, member secretary, *Law Commission* , has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated "*if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System".*

12. *Dynamic form of cyber crime-*

Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "*In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind**." * The* *(decreativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases. * *

13. *Hesitation to report offences*-

As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the *Delhi time theft case*. "The police are a powerful force today which can play an instrumental role in preventing cybercrime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business."*0 * This attitude of the administration is also revelled by incident that took place at *Merrut and Belgam*. (for the facts of these incidents refer to naavi.com. For complete realisation of the provisions of this Act a cooperative police force is require.

14. Time limitation-

Chapter eight of the ICT Act creates a cyber tribunal to adjudicate of cybercrimes. The judge of the tribunal will complete the judgment procedure within 6 month of filing the case. The judgment will be given within 10 days from the date of finishing examination of witness or evidenc or hearing.

* ** * I want to conclude in the following way* *that if we look upon the present context of our country we easily notice some drawbacks of existing cyber related law.Ruling govt. desire to digitalise Bangladesh. The precondition of satisfying vision 2021is to ensure cyber