Cyber Laws, Issues and Challenges- A thought starter

By

Naavi

India entered the regime of regulated Cyber Space on 17th October 2000 when Information Technology Act 2000 (ITA 2000) was notified. ITA 2000 for the first time gave legal recognition to electronic documents and a system of authentication of electronic documents similar to signatures in paper economy, called "Digital Signature". Together the recognition of electronic documents and digital signature enabled valid contracts to be entered with the use of only electronic documents. Additionally, ITA 2000 defined certain offences under Chapter XI and contraventions that impose civil liability under Section 43 of ITA 2000. The third most significant aspect of ITA 2000 was the setting up of two judicial authorities namely the "Adjudicating Officer" and the "Cyber Appellate Tribunal" to redress the grievances arising out of contraventions of ITA 2000 and provide civil compensation to the victims under a system which was not bound by the civil procedure code within a 4 to 6 month's time. A forgotten element of ITA 2000 was an inbuilt mechanism for review through the Cyber Regulations Advisory Committee which was a mandatory consultative body for framing rules and suggesting amendments.

Following the Baazee.com case in December 2004 where Section 67 of ITA 2000 was invoked along with Section 85 to charge the CEO of bazee.com of an offence, the industry brought pressure on the Government to undertake a review of ITA 2000. After some eventful 3 years and at least two different versions were recommended and rejected, the 26/11 Mumbai attack prompted the Government to show some urgency in passing amendments to ITA 2000 through the ITA 2000 amendment act 2008. Since the amendments were passed in the aftermath of a major terrorist attack, the amendments had a distinct "Information Security Flavor" and the new amended Act (ITA 2008) was born. This version became effective from 27th October 2009 when it was notified with a set of rules under Sections 69, 69A, 69B and 70A. A draft rule under Section 70B was released for debate and is now held back. In April 2011, a further set of draft notifications under Sections 43A and 79 has been released along with a draft regulation for Cyber Cafes and draft regulation for E Governance delivery under Section 6A.

Between 2000 and 2011, several developments have occurred in the Indian Cyber Space scenario where the provisions of the Act have been put to test. Certifying Authorities have come into existence after 2002, Adjudicating officers have come into existence since 2003 and Cyber Appellate Tribunal came into existence in 2007. The legal and judicial infrastructure for Cyber Crimes is therefore available. Police on the other hand have been training their personnel, setting up several Cyber Crime Police Stations and registering Cyber Crime cases.

This note examines briefly some of the issues and challenges in this context from the perspective of the Citizens.

Certain Issues Requiring Discussion are:

1. Is ITA 2008 capable of recognizing crimes that we see every day in Cyber Space?
2. Are our Police responsive to public when a complaint is made?
3. Is our Cyber Judiciary system ready to deliver the promise of ITA 2008?
4. Are "Intermediaries" and "Corporates" co-operative with the law enforcement?
5. Are generating expertise in cyber law and cyber forensics?
6. Are Cyber Laws being misused for Internet Censorship? Privacy Invasion?

1. Is ITA 2008 capable of recognizing crimes that we see every day in Cyber Space?

Cyber Crime is an evolving field. As and when technology moves new types of misuse surface. It is not possible for law to exactly identify different types of crimes and suggest remedies.

Hence Cyber Law has to describe offences only in general terms. This means that "incidents" need to be "interpreted" and mapped to different offences mentioned in the Act.

Description of offences in ITA 2000 was more generic than in ITA 2008. Under ITA 2008 (Sec 66), "Diminishing the value or utility of information residing inside a computer by any means" was recognized as an offence. This was broad enough to fit any offence involving electronic information.

To the extent this description remains a part of ITA 2008, except for the addition of the words "dishonestly" and "fraudulently", it is possible to interpret most offences using an electronic document under ITA 2008.

However, in ITA 2008, there is an attempt to add many sections to cover offences which can be covered under the above generic definition. As a result there is an overlap of some sections.

Introduction of Sec 66A (Covering offences using e-mails), Section 66F (Providing life imprisonment for Cyber Terrorism), Section 67B (providing a more stringent provision for Child Pornography), Section 66B (retention of stolen computer devices) have added

additional dimension to the description of crimes. Sections 67,67A along with Section 66E provide protection against obscenity.

Section 43A and Section 72A have provided teeth to "Data Protection". Section 43 is now integrated with Sec 66 and covers any offence where there has been an "Unauthorized Access" of a computer system resulting in wrongful harm.

Sec 67C is a powerful section that increases the responsibilities of companies and intermediaries and also adds special strength to Section 65 which was already in existence.

Sections 69,69A and 69B supported by Sec 70Bprovide enormous powers to Government agencies to enforce information security in the Cyber Space including households and private corporate sector. Sec 70 continues to provide powers to control information security in the Government systems.

Sections 71, 73 and 74 provide protection to the Digital Signature system. 66C and 66 D supplement the controls against misuse of identity in the form of password theft or otherwise.

There is an attempt to clarify on punishment for "Attempt to commit and offence" and "Assistance" as well as cognizability and compoundability.

Overall therefore the provisions of ITA 2008 regarding defining of Cyber Crimes are reasonably covered.

One omission is in the area of Cyber Squatting and domain name related disputes where there may be a need for creative interpretation of some of the existing provisions to bring offences under ITA 2008.

Making offences with not more than 3 year imprisonment as "Bailable" has been considered as one of the weaknesses in ITA 2008. However this can also be considered as a measure of protecting innocent victims from being harassed.

If this provision can be misused by offenders to manipulate evidences, it would be necessary for the Police to ensure that evidences are secured quickly.

Judiciary should also be responsive in certain cases to sanction "E Discovery" so that evidence is secured before they are erased.

Cyber Forensic capability being available within reach of Police at short notice therefore becomes a necessity in the emerging days.

2. Are our Police responsive to public when a complaint is made?

There is no doubt that Police are being trained in Cyber Crimes everywhere and it is yielding results. There is a reasonable awareness about Cyber Crimes in the Police. ITA 2008 has provided the power of investigation to the Inspectors and hence the task is huge and should continue.

However citizens are still not able to get their complaints registered with all Police Stations and the presence of "Cyber Crime Police Stations" in some places encourage some SHOs to avoid registration of cases. This status continues despite some directions given by the Police Chiefs in some States.

Registration of Cyber Crime complaints online and issue of acknowledgments followed by registration of FIRs is a burning need to ensure that Cyber Crimes are reported by public without hassles.

Some provisions of CrPC is often quoted as reasons why such innovation would not be feasible but solutions need to be found by the Police Chiefs to provide this facility as a measure of creating confidence in public about Cyber Crime mitigation.

A time has come for Police to create district wise Cyber Crime Expertise centers and let each Police Station function as Cyber Crime Police Station rather than having one Cyber Crime Police Station for the State. Such district centers can be equipped with adequate Cyber Forensic capabilities to ensure quick evidence capturing.

One other difficulty that Police face is the lack of support from Intermediaries such as Internet Service Providers, Mobile Service Providers, Web site owners etc. when some information required for investigation is called for. Google, Yahoo and others protect the criminals by their privacy protection policies and hinder quick investigation of crimes.

This requires a national level policy formulation and further debate as to how to get the sensitive information without sacrificing privacy protection.

3. Is our Cyber Judiciary system ready to deliver the promise of ITA 2008?

Cyber Judiciary system envisaged under ITA 2000/8 essentially wanted that civil disputes are resolved without the enormous delays that exist in the country's civil judiciary system. Hence though the powers of Civil Court were conferred on the Adjudicators and the Cyber Appellate Tribunal (CAT), these institutions were freed from being constrained by Civil Procedure Code and asked to follow the principles of natural justice.

Adjudication was structured as more of an "Enquiry" so that the complaint was not required to provide evidences and witnesses and proof as may be necessary in a normal Civil Court. The role of the complainant was only to report the incident and the Adjudicator was more responsible to gather evidences through an enquiry and investigation through Police.

Further the complainants were allowed to be represented by subject experts so that "Resolution" was the focus of the judicial bodies and not "procedures".

Also a time limit of 4 to 6 months was suggested for both the Adjudicator and the CAT to complete the process before the matter could reach the conventional judiciary at the High Courts as an appeal against the CAT.

ITA 2008 also ensured that CAT can be a multi member body, can sit anywhere in India and also provided for setting up of multiple CATs in the country.

The system of Adjudication and CAT as envisaged in ITA 2000/8 is therefore highly commendable and is an important instrument of making Cyber Law regime in the Country successful.

Whether the Cyber Judiciary system has been able to live up to the expectations of the people? .. is a matter which requires some study at this point of time.

The difficulties that are encountered in the Cyber Judiciary can be summarized as follows.

a) Adjudicators who are IT Secretaries are hesitant to take up additional responsibilities associated with Adjudication. Hence complainants are turned off (subject to exceptions in some States like Tamil Nadu) just like the Police Stations refuse to register Cyber Crime complaints.

b) Advocates familiar with the CPC are unable to accept the summary proceedings and the "Enquiry" nature of the proceedings at the Adjudication and find it difficult to adjust to the system. Gaining adjournments on flimsy grounds and taking unreasonable time for filing replies and counters every time is a strategy adopted by some counsels to delay matters. Since these are common in Civil Courts, there is a danger of the Cyber Judiciary system also going the Civil Judiciary way (as regards time required for completion of proceedings) unless the tendency is nipped in the bud.

c) Most of the participants are so tuned to CPC that they are unable to avoid being bogged down by procedures which may consist of application being made in a certain number of copies, in a certain format, with Court fee stamping been affixed, with

legal paper being used etc. and miss the essence of the "Principle of Natural Justice". The casualty in this process is the "Time Limit" for completion of the adjudication or hearing of the Appeal in CAT.

d) Coupled with the time delays is the issue of change of guard of either the Adjudicator or the CAT chief. By the time the incumbent comes to get a hang of Cyber Crimes and nuances of Cyber Crime judiciary, their term may come to an end and the learning curve starts again.

e) Most of the Cyber Judicial offices are yet to use Virtual conference tools as provided in ITA 2000 and accompanying rules so as to reduce the cost of litigation and also to reduce delays.

f) Substantial work is therefore required to ensure that Cyber Judiciary system lives up to the great expectations raised by ITA 2000/8.

4. Are "Intermediaries" and "Corporates" co-operative with the law enforcement?

Intermediaries and Corporates always look at law enforcement as an intrusion to their work and hence will try to avoid working with them even when the corporate interest itself is involved. Most of the time Crimes committed within the corporate network is not reported and when identified, the perpetrator is only eased out of the job and not handed over to the law enforcement even when it is necessary in the interest of the society.

Intermediaries in particular are store houses of investigative information and they are a big stumbling block in bringing cyber criminals to book.

ITA 2000/8 therefore makes corporates and intermediaries liable for civil and criminal penalties when their resources are used in the commission of a crime.

Though there is an element of opposition to the concept of "Due Diligence" amongst the corporate sector, this is the only way that cybercrimes can be reduced. Hence major IT service providers such as Internet and Mobile Companies, Banking and Share broking companies, E Commerce companies etc. need to implement information security from the perspective of preventing its users being saddled with liabilities.

There is a need therefore to make every intermediary undergo periodical ITA 2008 compliance audit and take reasonable precautions to prevent occurrence of Cyber Crimes within their domain.

This requires a change of heart in the commercially minded business entities to set aside some investment for information security and consumer education.

5. **Are we generating expertise in cyber law and cyber forensics?**

   In order to create the right pool of talents in Cyber Law and Cyber Forensics, the curriculum in our education needs to be geared up to

   a) Create awareness of Cyber Crimes at the High School level

   b) Introduce Cyber Laws in the Curriculum in graduation level

   c) Introduce Information security in the curriculum at the Technical and Management education

6. **Are Cyber Laws being misused for Internet Censorship? Privacy Invasion?**

   The recent notification under Section 79 issued by the MCIT is a step in the direction of defining "Due Diligence". However the notification has come for severe criticism since it can be misused as a means of Internet Censorship. The fear is borne out of several cases in the past where the power of the executive to issue instructions to block websites has been used without proper checks and balances.

   There is need to ensure citizen participation in implementation of sensitive controls such as blocking of websites to avoid the provisions being misapplied.

The above is a set of initial thoughts that can be explored and debated by experts.

Na.Vijayashankar

www.naavi.org

+919343554943