Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study *

N. S. Nappinai
nappinai@gmail.com

Abstract. India owes a lot to the exponential growth of the Information Technology service Industry over the last 15 years. Though India got its first codified Act in the Information Technology Act ("IT Act), in the year 2000, the IT Industry and in fact all businesses with cross-border obligations have been left crying themselves hoarse for more! The Indian Legislature has now passed a mish – mash legislation in December 2008, which clearly demonstrates the appeasement policy adapted to meet the various and in some instances divergent interests of the Industry and the Government. The scope of this paper is to highlight some important provisions of the cyber criminal laws in India relating to data protection, privacy, encryption and other cyber crimes and the extent to which the said provisions arm the enforcement authorities to combat not just existing but emerging trends in Cyber Crime.

1. Introduction

The general laws in India were drafted and enacted in the 19th century[1]. Whilst each of the general laws have undergone modifications and amendments, the broad and underlying provisions have withstood the test of time, including unimaginable advancements in technology, which speaks to the dynamism of the General laws. The general laws referred to in this Article are the Indian Penal Code, 1860 ("IPC"), which is the general penal law of India and the Indian Evidence Act, 1872 ("Evidence Act"), the general law pertaining to admissibility of evidence in civil and criminal trials. The manner in which trial of criminal cases are to be conducted is dealt with under the Criminal Procedure Code, 1973 ("Cr. P. C").

India got its first codified Act in the Information Technology Act, 2000 ("IT Act), which fell far short of the Industry's requirements to meet global standards. The focus if the IT Act was however recognition of electronic records and facilitation of e -commerce. Barely ten sections were incorporated in the IT Act to deal with Cyber Crime[2]. At the time when the IT Act was passed several acts deemed to be illegal in most jurisdictions including virus attacks, data theft, illegal access to data / accessing and removal of data without the consent of the owner, etc., were listed as civil penalties under the IT Act[3]. The IT Industry continued to rely on self –regulation and contractual undertakings to appease its global clients, as it had done before the passing of the IT Act. The primary offences under the IT Act were:

- Tampering with source code[4];
- Deleting, destroying or altering any data on any computer resource with mala fide intent to cause wrongful loss or to diminish its value[5];
- Publishing or transmitting pornographic material through a computer resource;
- Provisions pertaining to encryption technology, the right of the Government authorities to intercept and decrypt such data and to call upon any entity or individual to decrypt such data were also included in the IT Act. Certain acts affecting the integrity and sovereignty of the nation were classified as offences.

The saving grace of the IT Act were the amendments carried out to the IPC and Evidence Act, which to some extent provided for prosecution of rampant offences like the Nigerian Scams[6], Phishing and other Banking

* This paper was originally published in Kierkegaard, S. (2009) Legal Discourse in Cyberlaw and Trade. IAITL.
[1] The Indian Penal Code, 1860 & the Indian Evidence Act, 1872;
[2] The phrase "Cyber Crime" is not defined in any enactment in India. This to some extent leads to some confusion whilst enforcing the various provisions spread over the Special and general laws, as more fully set out in the Article;
[3] S.43 of the IT Act;
[4] S.65 of the IT Act;
[5] S.66 – misleadingly termed "Hacking" under the IT Act;

frauds may be prosecuted. Cyber Crime prosecution was however not resorted to in many instances due to lack of awareness (amongst both the victims and the enforcement authorities) about the applicability of such general Laws to cyber crimes (like Phishing). To add to this, administrative delegation of powers treated offences under the IT Act differently to those falling under general laws!

Further, crimes like data theft; illegally accessing / removal of data; virus attacks etc., could not be prosecuted due to the lack of relevant penal provisions. S.66 of the Act misleadingly titled "hacking" is one of the most misused and abused provisions in India. Recently i.e., in September 2009, the Delhi High Court[7] has quashed the criminal proceedings initiated in or about July 2005, under S.66 of the IT Act by M/s. Parsec Technologies Ltd., against some of its former employees, who left and started their own Company, holding that the continuation of the proceedings would amount to abuse of process of law. Likewise the IT Act did not provide sufficient recourse for women and child victims of cyber crimes like Cyber Stalking and paedophilia.

Controversy has dogged the IT Act from its inception. The Ministry of Information Technology prepared and posted proposed draft amendments to the IT Act in 2005. In 2006, the IT Bill with substantial changes brought about as a result of the objections to the proposed amendments of 2005 was tabled before the Parliament.

In December 2008 as a knee–jerk reaction to the November 2008 terror attacks in Mumbai, India, the Information Technology (Amendments) Act, 2008[8] ("ITA, 2008") was hastily tabled before the Parliament and was passed hastily and without any debate whatsoever. Unlike the IT Act of 2000, the focus of the new ITA 2008 is clearly on Cyber Terrorism and to a significant extent, Cyber Crime.

This paper deals with some important provisions of ITA, 2008 relating to data protection, privacy, encryption and cyber crime and to what extent it arms one against emerging trends in Cyber Crime.

2. Definitions

Some noteworthy amendments in the definition sections include:
The replacement of the word "Digital" with the word "Electronic", which makes the IT Act more technology neutral and expands its applicability beyond just the digital medium.

- Inclusion of cell phones, personal digital assistants and other such devices in the definition of "Communication Devices" broadens the scope of the statute.
- The modified definition of "Intermediary" includes all service providers in respect of electronic records again broadens the applicability while inclusion of Cyber cafes in the definition of Intermediaries removes the need to interpret the statute.

The extensive definition of "cyber security" as including protection of both data and the equipment from unauthorized access, use, disclosure etc., is another vital inclusion that impacts the new Data Protection provisions included under the ITA, 2008. The relevance of these definitions, where applicable are set out below.

3. Data Protection

The IT industry has been lobbying for a law to protect Data and the new legislation has addressed the industry's demands to a certain extent particularly since Mphasis Limited, a Pune based Company suffered the notoriety of puncturing the Indian BPO fairy tale in April 2004, when some of its employees stole confidential credit card information of clients and used it to siphon substantial amounts. Apart from highlighting the security lapses within the Company, this case also brought to the limelight the lack of suitable Data Protection Laws in India. Several cases have now been reported where former employees are accused of data theft and misuse of Confidential and proprietary Information and data. In one instance[9], a BPO Company purportedly closed down due to rampant data theft. The Indian Legislature's response to the hue and cry raised is the transposition of certain civil penalties into criminal offences and the addition of one section under civil penalties as set out hereunder:

---

[6] Such scams are more rampant since last year, where emails claiming to give out winnings in lotteries; winnings for selected email ids (the latest twist is the scam of claiming payments for handing over winnings for selected mobile numbers through SMS messages) etc., and asking for deposits and payments for customs clearance etc.,

[7] The Apex Court of a State in India;

[8] Bill No. 96 – C of 2008 passed by the Lok Sabha on December 22, 2008 and to which the President's assent was given on February 5, 2009;

[9] In the instance of M/s. Acme Tele Power Limited, a BPO;

The only provision under the IT Act for data protection was S.43[10], which only imposed Civil Penalties in the event of the commission of certain acts without the permission of the owner or person in charge of the computer or computer systems such as: (i) securing access (without permission); (ii) downloading or copying of data stored in a computer or computer system; (iii) introducing computer viruses; (iv) damaging computers and or data stored therein; (v) disrupting computers; (vi) denial of access; (vii) abetting such acts; or (viii) illegal charging for services on another's account.

S.43A has now been added under the ITA 2008 to address the data protection requirements of the Industry. S.43A stipulates that any "Body Corporate[11]" possessing, dealing with or handling any "sensitive personal data or information[12]" in a computer resource it owns, controls or operates, is liable for negligence, if it fails to maintain "reasonable security practices and procedures[13]" and thereby causes wrongful loss or wrongful gain to any person. What amounts to reasonable security practices and procedures remains to be finalized by the Central Government.

Apart from the above addition under Civil Penalties, the Civil wrongs set out under S.43 of the IT Act have now been qualified as criminal offences under the ITA 2008 under S. 66[14]. A reverse transposition has further been carried out under the ITA 2008 of two criminal provisions from the IT Act (S.66 and S.65) as civil penalties under S.43 (i)[15] & S.43 (j)[16], respectively.

Any act set out under S.43, if committed "dishonestly or fraudulently", would amount to a criminal offence, punishable with punishment of up to three years or fine of a maximum of Rupees Five Lakhs or both, under the ITA 2008. Though S.66 of the IT Act has purportedly been deleted, the addition of S.43 (i) under the ITA 2008 has in effect resulted in the retention of the contentious S.66 of the IT Act. However retention of S.65 of the IT Act without any modification despite its transposition into S.43 appears to be a tautology, which could be due to oversight.

S.66B inserted by the ITA, 2008 is on the lines of similar provisions in the Indian Penal Code ("IPC"), which provides for punishment of the receiver of stolen property. S.66B makes the receipt or retention of a stolen computer resource or communication device punishable with imprisonment up to three years or with fine up to Rupees One Lakh or both. Whilst S.66B may seem to also apply to hardware, which is also covered under the IPC, the term "computer resource" is defined under the IT Act as a "Computer, computer system, computer network, data, computer database or software." The extension of the above provision to the receiver of stolen data, software etc., may prove to be substantially useful when faced with issues of Corporate Espionage.

4. Further analysis of the data protection legislation

Although the data protection provisions introduced by the ITA, 2008 (as described above) may not comprehensively address the industry specific requirements applicable to data providers and handlers; nevertheless this is an important head start towards introduction of specific data protection legislation in India, which is absolutely essential in today's business environment.

One of the important outcomes of the ITA, 2008 amendments is the clarity on whether Data theft is considered a criminal offence. Commission of acts provided in S.43 to 66 dishonestly or fraudulently, clearly implies "Data Theft" as an offence in such instances. However these acts would amount to a punishable offence only if such data is "downloaded, copied or extracted" from a computer resource. Therefore it may be argued that the provisions of S.43 (b) are not inclusive, as they do not provide for removal of data through uploading. Criminal provisions give rise to liability only in cases of unambiguity. If a provision has to be applied through interpretation, then such interpretation, which favours the Accused, would have to be applied.

---

[10] Chapter IX - "Penalties & Adjudication", (which has also been amended in ITA, 2008, as "Penalties, Compensation & Adjudication");

[11] Body Corporate" is defined to mean "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities";

[12] "Sensitive personal data or information" is not specifically defined in the ITA, 2008 and is left open to be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

[13] "Reasonable security practices and procedures" is defined as "security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem it;"

[14] The existing S.66 under the IT Act has been deleted;

[15] S.43 (i): "destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means";

[16] S.43(j): steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage";

With the addition of S.43A by the ITA, 2008, the onus of implementing "Reasonable Security Practices" is on the business entity. Whilst this may be a known liability that parties agree upon, unsuspecting companies or firms may get mulcted with liability if duties and obligations are not specified, as the Central Government guidelines will then become applicable. As of now, violations under S.43 A are however not criminal offences.

4.1 Confidentiality & Privacy

India was shocked out of its complacent conservatism due to the widespread circulation of a MMS clip shot by a Delhi schoolboy[17]. This case took an unexpected twist when this clip was circulated on Bazee.com and its Chief Executive Officer of American origin was arrested. S.66E has now been introduced under the ITA, 2008 for the protection of physical or personal privacy of an individual. This section makes intentional capturing of the images of a person's private parts without his or her consent in any medium and publishing or transmitting such images through electronic medium, a violation of such person's privacy punishable with imprisonment of up to three years or with fine up to Rupees Two Lakhs, or both.

A case of posting of the personal information and obscene material on a Yahoo! Site was touted as the fastest trial and conviction of a cyber crime case in Chennai[18]. It appears that this conviction has recently been reversed. S.72 A of the ITA, 2008 now explicitly provides recourse against dissemination of personal information obtained without the individual's consent through an intermediary or under a services contract, with intent to cause wrongful loss or wrongful gain. The maximum punishment prescribed for this offence is three years imprisonment, or fine up to Rupees Five Lakhs or both.

Service providers on the Internet, social networking sites, Companies, firms, individuals and other intermediaries ought to now be careful in the collection, retention and dissemination of personal data. Interactive websites and P2P site operators also have to be extremely careful to ensure that the provisions of S.66E & S.72 A are not violated.

4.2 Other Cyber Crimes including Cyber Terrorism

Provisions to combat cyber frauds have now been introduced under the ITA 2008. However certain issues relating to protection against banking frauds such as Phishing, money transfers through online hacking, email frauds and cyber squatting (including through wilfully misleading domain names) to name a few have not been addressed separately in the ITA, 2008, even though these are significantly increasing problems.

S.66C inserted by the ITA, 2008 makes dishonest or fraudulent use of a person's electronic signature or identity, password or any other unique identification feature punishable as theft with imprisonment of up to three years and fine up to Rupees One Lakh.

S.66D inserted by the ITA, 2008 makes cheating by personating through a computer resource punishable with imprisonment of up to three years and fine up to One Lakh Rupees. It may be noted that S.419 of IPC already provides for punishment for cheating by personating but does not provide for the maximum fine imposable.

In addition to S.67 of the IT Act, S.67A and S.67B have been included by the ITA, 2008 *inter alia* to combat child pornography. S.67A makes transmission of a sexually explicit act or conduct punishable and S.67B makes publishing and transmission of child pornography an offence, punishments for which range from five to seven years and fine. Several exceptions have also been set out to S.67 and S.67A, including for depictions in any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form.

Further, S.67C introduced by the ITA, 2008 imposes liability on Intermediaries for retention and production of information. However the duration, manner and formats of retention of such information are still subject to prescription by the Central Government. This section appears to be directed mainly against Cyber Cafes and has already been subject to dissension. Failure to comply with such requirements is punishable with imprisonment up to three years and also fine.

4.3 Observations on the Cyber Crime provisions under the ITA, 2008

S.43 was included in the IT Act, 2000 to address certain kinds of illegal acts. However, the Legislature has not looked beyond S.43 to address recent trends in Cyber Crimes and for dealing with such issues.

[17] The Delhi Public School student had allegedly shot video clippings on his mobile of his amorous activities with his classmate in 2004;

[18] State of Tamil Nadu Vs. Suhas Katti (2004);

S.66 of the IT Act, under the heading "Hacking" which was misleading was criticized for its ambiguity and for the possibility of abuse. However, whilst the proposed amendments sought for its deletion, this section has been transposed to not only being applicable as a civil penalty but is also retained as a criminal offence. With the retention of S.66 of the IT Act, one of the main issues that need to be addressed is the criminality of actions resulting in "diminishing of value" of any information residing in a computer resource. Even if the law – makers thought fit to retain this provision, its use and abuse since 2000 ought to have been evaluated when re-defining this provision.

S.66C only addresses some kinds of cyber frauds and not all such frauds committed without using digital or electronic signatures. Further S.66D may be considered redundant in the light of the amendments made to the IPC after the enactment of the IT Act in 2000, save and except for the maximum fine imposable under the ITA, 2008.

S.67A is a much – needed introduction to the IT Act and would help in combating the pernicious offences of child pornography as observed in some recent shocking incidents involving school children.

Several new provisions have been introduced under the ITA 2008 to combat cyber Terrorism. These provisions appear to be a necessary and welcome addition though there are apprehensions about their abuse and whether the Government authorities are well equipped to handle and protect the information, acquired by it in compliance with such provisions.

S.66A inserted by the ITA, 2008 is an essential provision from the perspective of combating Cyber Terrorism and to address several instances of cyber stalking, cyber harassment, etc. However this provision can also be easily abused. S.66A provides for punishment of three years and fine against any person found guilty of: (i) sending information through a computer resource or devise, which is grossly offensive or of menacing character; (ii) false information intended to annoy, inconvenience, deceive or mislead the addressee or recipient about the origin of such message; or (iii) endanger, obstruct, insult, injure, intimidate or to cause enmity, hatred or ill will. This would not only help the police against anonymous and false messages etc., and harassed individuals, but also corporate bodies, which could rework their internal policies in consonance with this provision.

S.66F directly addresses the issue of cyber terrorism. Acts intended to: (i) threaten the unity, integrity, security or sovereignty of India; (ii) to strike terror in the people or any section of the people by denial of access, hacking and virus attacks; and (iii) by such means does or may cause death or injuries to persons or damage to property or disrupts supplies or services essential to the life of the community; or (iv) adversely affects the critical information infrastructure; is the commission of Cyber Terrorism, the punishment for which ranges from imprisonment from three years to life and fine depending upon the seriousness of the crime.

4.4 Encryption & Data Privacy

Mid 2008, customers in India thought twice about buying Blackberry phones – no reflection on the performance of the phones but due to a sudden conflict between the Department of Telecommunications of the Indian Government ("DoT") and Research in Motion ("RIM") Blackberry Services. DoT requested RIM to share its encryption codes with the department, stating security concerns over data transmitted through email services on Blackberry phones or to set up servers in India and permit DoT to monitor such transmissions. After several rounds of talks the Government of India dropped its request reversing its stand on the issue of a security threat.

The Indian Telegraph Act, 1885 vests extensive and absolute power on the DoT *inter alia* to deal with, monitor and regulate transmission of messages within India. These provisions therefore stand automatically extended to transmission of encrypted Data also. The Guidelines issued by the DoT for transmission of encrypted data and the ISP license requirements permits transmission of encrypted data of 40 bit key length in RSA algorithms or its equivalent in other algorithms without having to obtain permission from the Telecom Authority. However, if encryption equipments higher than this limit are to be deployed (which would be the case for most encrypted data), individuals/groups/organizations require prior written permission of the DoT and may be further called upon to deposit the decryption key, split into two parts, with the DoT. These provisions appear to have prompted the Blackberry case. Now in addition to the above powers vested in the Telecom Authority of India, certain provisions have been added under the ITA 2008 (as set out hereunder), which further strengthens the hands of the Telecom Authority in India.

S.69 of the IT Act, which dealt with encrypted data has been replaced with a new S.69, which empowers the Central Government or a State Government through their authorized officers to intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. These powers may be exercised for reasons set out in S.69 including in the interest of the sovereignty or integrity of India, defence, security of the State, or even for preventing commission of any cognizable offence or for investigation of any offence. The only restraint in exercising such powers is the necessity of maintaining written records of such actions. The additions to S.69 and inclusion of new provisions under S.69A to S.69C under the ITA 2008 may be subject to criticism and concern.

S.69A empowers the Central Government or any of its authorized officers to block or cause to be blocked access by public of any information generated, transmitted, received, stored or hosted in any computer resource.

Under S.69B, the Central Government may, through its authorized agency, monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource for enhancing cyber security and for identification, analysis and prevention of intrusion or spread of virus in the country. Intermediaries have to provide such data and assistance as sought by the authorized agency and failure to extend such assistance is punishable with imprisonment up to three years and fine.

S.70A and S.70B provides for notification of any Government organization as the national nodal agency for Critical Information Infrastructure Protection and notification of any Government organization as the Indian Computer Emergency Response Team, respectively.

S.84A gives extensive powers to the Central Government to prescribe encryption methods to ensure secure use of the electronic medium and for promotion of e-governance and e-commerce.

4.5 Other Relevant Provisions

S.77A of the ITA, 2008 provides for compounding of offences under this Act, other than: (i) offences punishable with life or imprisonment for a term exceeding three years; (ii) in cases of enhanced punishment; (iii) those affecting the socio economic conditions of the country; or (iv) offences against a child below the age of 18 years or a woman. Whilst some of these exceptions appear to be precise and appropriate, certain others appear ambiguous i.e., exception on the grounds of socio economic conditions.

S.77B makes all offences punishable with three years and above imprisonment cognizable and bailable, notwithstanding the provisions of the Indian Code of Criminal Procedure, 1973.

With the increase in cyber crimes amounting to offences under the ITA, 2008, the power to investigate offences under this Act has been vested with an Inspector instead of the Deputy Superintendent of Police. This may reduce the confusion relating to jurisdiction for registering of offences. Further this would entail commencement of extensive and immediate cyber law awareness measures by the investigation agencies throughout India. There is however anxiety in the minds of the industry about the ability of the police official of such rank being able to handle such additional responsibility.

S.79 has been modified by the ITA, 2008 to restrict the liability of an Intermediary under this section to specific instances, i.e., if he provides access to communication systems for transmission or temporary storage of third party information, data or communication links made available or hosted by him. The Intermediary should however observe due diligence and comply with the prescribed guidelines, while discharging his duties.

S.85 of the IT Act, which imputes vicarious liability in case of offences by companies, has been retained in its original form despite criticism by different industry sectors. As most of the offences under the IT Act have been made cognizable, and with the increase in the number of offences added under the ITA, 2008, this provision may be cause for concern.

5. Conclusion

Though the ITA 2008 has been passed by the parliament, the Amended Act is still not the law of the land. The ITA 2008 will come into effect only from the date notified by the Government of India[19], which still remains pending as on the date of publication of this paper.

Introduction of several provisions in the IT Act by the ITA, 2008, relating to data protection, are extremely essential in today's business environment as several Indian companies providing services to or in conjunction with foreign entities handle large amounts of data that are accessed and/or processed by their employees. Such cross border exchange / transmission of Data further mandates compliance with the provisions of foreign enactments on Data Protection[20]. The increased accountability of data handlers and data aggregators and the enhanced punitive measures, therefore meets such requirements to some extent.

The existing provisions along with the additional / revised provisions under the ITA, 2008 provide for criminal prosecution and stringent monetary penalties that are likely to act as effective deterrents. Whilst some inclusions in the ITA 2008 have been subject to criticism, the amendments and additions made to the IT Act are

[19] S.2 of the ITA, 2008;

[20] For instance Schedule I, Part I, Article 8. of the UK Data Protection Act, 1998 stipulates that "Personal data shall not be transferred to a country or territory outside the European Economic Area ***unless that country or territory ensures an adequate level of protection*** for the rights and freedoms of data subjects in relation to the processing of personal data" (Emphasis Added).

expedient and much awaited additions. Absence of effective provisions to combat offences like Cyber Stalking and cyber squatting are avoidable loopholes, which one hopes will soon be rectified. One could safely conclude that whilst the ITA 2008 is still work in progress, it is definitely headed in the right direction.