THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
VOLUME 7, 2011

NEW CRIMES UNDER THE INFORMATION TECHNOLOGY (AMENDMENT) ACT

Amlan Mohanty[*]

ABSTRACT

This paper delineates the legislative response to cyber crime in India with an analysis of the Information Technology (Amendment) Act, 2008 focussing on the new crimes introduced by the amendment, on the touchstone of cyber crime legislative standards across jurisdictions. Thus, a brief look at the jurisprudential basis for criminalisation of cyberspace activities has been undertaken, following which, the new crimes have been examined section-wise. The paper uses the theoretical framework set out in the first section to probe the various problems that the Amendment Act poses in light of bad drafting and lack of understanding in the area.

TABLE OF CONTENTS

[*] The author is a fourth year student at the National Law School of India University, Bangalore. He may be contacted at mohanty.amlan@gmail.com.

I. INTRODUCTION

On December 22, 2008, the Information Technology (Amendment) Act, 2008 was passed by the Lok Sabha with almost no discussion whatsoever.[1] The Bill had been introduced in 2006 and in the wake of the terrorist attacks in Mumbai on November 26, 2008, the Act was passed as a reactionary measure.[2] The fact that the Bill was not discussed prior to it being passed is clear in its drafting. In some places, apart from being just poorly drafted, it is also vague and criminalises offences without defining the scope of the activity that could classify as criminal.

The Bill was passed by the Rajya Sabha on December 23, 2008, and received Presidential assent in early 2009. However, even after this, the Act did not come into force until October 26, 2009, when it was notified by the Central Government.[3] The Act though passed in such a rush did not come into effect until a year later. This time could have been used to discuss the Bill and address the various problems with it.

This essay looks at the new offences introduced by the Amendment Act as a legislative response to the increasing threat of cyber crime in India today, and analyses these offences in light of similar provisions in other jurisdictions. The essay first looks at the jurisprudential basis for criminalisation of activities over the internet. In this section, the essay looks at self-regulation as an adequate means of policing the internet and whether government intervention and criminalisation of cyberspace activities is necessary. The section concludes with a brief framework which is used in the analysis of the provisions in the rest of the essay. Various new offences introduced by the Act have then been studied section-wise, using the framework as explained in the first section. The scope of this essay is thus limited to the new crimes introduced by the amendment and determining the adequacy of the legislative response to the growing need

---

1 Pavan Duggal, *IT Act Amendments – Perspectives by Mr. Pavan Duggal*, CYBERLAWS.NET, http://www.cyberlaws.net/new/pd_on_ITAmendments.php (last visited Jan. 23, 2010).

2 Karen M. Sanaro & Christyne Ferri, *India's New Information Technology Law Impacts Outsourcing Transactions*, ST. B GA., June, 2009, http://www.technologybar.org/2009/06/indias-new-information-technology-law-impacts-outsourcing-transactions/ (last visited Jan. 23, 2010).

3 Press Release, Ministry of Communications & Information Technology (October 27, 2009), PIB.NIC.IN, http://pib.nic.in/release/release.asp?relid=53617 (last visited Jan. 23, 2010).

for a legislation that brings within its fold emerging forms of cyber crime. The essay concludes by looking at the various problems that the Amendment Act poses in light of bad drafting and lack of understanding in this area.

II. REGULATION OF CYBERSPACE

A. Need for regulation of cyberspace activities

A good starting point for an illuminated argumentation on the criminalisation of activities in cyberspace is the aspect of regulation of these activities itself and associated questions of its desirability, necessity and feasibility. The rhetoric of the cyber libertarians, seeking self-regulation of the internet, while challenging perceived essentialities for any kind of regulation, like territorial boundaries, real relationships and notions of property, is firmly grounded on the assertion that cyberspace is capable of being regulated through the creation of institutions and mechanisms for the regulation of conduct in cyberspace through the formulation of community based rules that are constituted, decreed and enforced by its participants without necessitating state intervention. On the other hand, those demanding government regulation stress on the inadequacy of such a system to combat instances of grievous criminality. A closer look at the contentions of both parties provides an academic space for a discussion on the criminalisation of cyberspace activities and a canvas to contextualise the nature of offences introduced by the amendment.

The cornerstone of the self-regulation theory is that the absence of government involvement in regulatory mechanisms does not result in *cyberanarchy* and suggests that the application of geographically based conceptions of legal regulation to cyberspace activities makes no sense at all, and further, that cyberspace participants are better positioned than the government to design a comprehensive set of rules that are cheaper to enforce and are practically sound.[4] The justification for such an idealistic viewpoint is buttressed by moral considerations often expressed by the participants of cyberspace who unequivocally express their objections to being disciplined by orders of the government and declare the space that they have created for themselves to be independent of the tyrannies of government order.[5]

---

4 Jack L. Goldsmith, *Against Cyberanarchy*, 65(1) U. CHI. L. REV. 1199 (1998).

5 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION, http://homes.eff.org/~barlow/Declaration-Final.html (last visited December 5, 2009).

Entrusting the internet community with the power to create legal rules and institutions will overcome inherent difficulties associated with geographical determinacy and territorial enforcement and evolve into a mechanism to govern a wide range of new phenomena that have no clear parallel in the non-virtual world,[6] thus saving the legislature the time and energy to draft laws to deal with such situations. The proponents of self-regulation draw credibility from their claim that State laws enacted to deal with cyberspace activities have been unsuccessful,[7] and that existing laws and methods of lawmaking are inadequate,[8] and so, the internet should be self-regulated. The underlying principle entrenched in these views is that cyberspace is the antithesis of regulations and the impracticalities of regulation by external forces including law enforcement forces are too compelling to make such an attempt. The dispensability of government intervention is intimately twined with the complicated nature of social relationships in cyberspace, wherein criminal acts are reprimanded by third party Internet users who impose community defined sanctions on offenders as a form of punishment akin to State law enforcement mechanisms that seek to penalise the same crimes by utilising additional State resources with less than desired effects.

B. Need for criminalisation of offences in cyberspace

To highlight the limitations of self-regulation, or the opposite parties' contentions in this case, would be to make a case for the criminalisation of offences in cyberspace through State intervention, a position several scholars have taken with the advent of serious offences and increasing criminality on the internet such as paedophilia, cyber frauds, data theft, impersonation and cyber terrorism.[9] The typical self-regulation punishment model is centred on banishment from the group,[10] a procedure for social control that appears lenient and lacking in deterrence value as opposed to criminal sanctions imposed by the State to deter any destructive or anti-social conduct in cyberspace. It appears

---

6 David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 (5) STAN. L. REV. 1367 (May, 1996).

7 Jason Kay, *Sexuality, Live Without A Net: Regulating Obscenity And Indecency On The Global Network*, 4CAL. INTERDISCIPLINARY L.J. 355 (1995).

8 Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations By Internet Services Providers: How To Stop That Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber*, 9 HASTINGS COMM. & ENT. L.J. 661-664 (1997).

9 S.V. JOGA RAO, LAW OF CYBER CRIMES AND INFORMATION TECHNOLOGY LAW 10 (2004).

10 Based on terms and conditions of access and use, imposed by service providers, commonly referred to as '*netiquette*'.

that the stream of anti-governmentalism has been laid to rest in view of the fact that the internet has quite simply become too mainstream, and being the preferred platform for electronic commerce, the need for governmental regulation cannot be ignored.[11] Perhaps the greatest argument in favour of criminalising unlawful conduct on the internet is its distinctiveness from territorial crime. The very fact that cyber crimes are easier to learn how to commit, require fewer resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present in it and the fact that they are often not clearly illegal[12] make criminalisation of such conduct not only important, but essential. The conclusion that must be reached is that the State must step in with some level of regulation of cyberspace.[13]

C. Types of offences to be criminalised

An analysis of the new crimes introduced by the IT (Amendment) Act on the touchstone of cyberspace conduct sought to be criminalised by statutes and conventions around the world would help in determining the suitability and stringency of the new sections in the Indian scenario.

There are essentially four main types of conduct that a domestic legislation should penalise - (1) offences against the confidentiality, integrity and availability of computer data and systems, (2) computer-related offences with the intention to defraud, (3) content related offences, and (4) offences related to infringements of copyright and related rights.[14] In order to acquire a jurisprudential understanding of cyber crimes in general, and to gain a critical insight into the nature of offences introduced by the amendment and whether they serve the function expected of them, it is important to comprehend *why* these particular forms of conduct are criminalised across jurisdictions. Further, it is also essential to understand the range of unlawful conduct that involves computers. With

---

11 Robert Shaw, *Should the Internet be Regulated*, 2(4) IFO INSTITUTE FOR ECONOMIC RESEARCH AT THE UNIVERSITY OF MUNICH 42 (October, 2000), http://www.ifo.de/DocCIDL/Forum401-pc1.pdf (last visited December 14, 2009).

12 MACCONELL INTERNATIONAL, CYBER CRIME... AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION, (World Information Technology and Services Alliance, 2000), http://www.witsa.org/papers/McConnell-cybercrime.pdf (last visited December 1, 2009).

13 David S. Wall, *Cybercrimes: New Wine, No Bottles?*, *in* INVISIBLE CRIMES: THEIR VICTIMS AND THEIR REGULATION (Pam Davies, Peter Francis &Victor Jupp eds.,1999).

14 European Convention on Cybercrime, Guidelines for member states, 2001, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (last visited December 12, 2009).

the first, second and fourth type of conduct, private individuals may not be able to detect and proceed against the perpetrators and it therefore falls upon the State to intervene and impose criminal sanctions. It is necessary to criminalise acts falling within the third category as they are offences that shock the conscience of society and threaten public morality.

III. NEW CRIMES UNDER THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

Having erected a framework for comparative scrutiny of the Information Technology Act, 2000 (hereinafter, "IT Act") with cyber crime legislative standards across the world, it is plainly visible that the IT (Amendment) Act, 2008 (hereinafter "ITAA") was introduced to tackle unresolved cyberspace issues such as internet fraud, pornography, data theft, phishing etc., that were not explicitly covered under the old legislation but are at the heart of internet activity, nevertheless.

A. An overview of changes under section 66 and 67

Under the old act, criminal offences were specified under Sections 65,[15] 66[16] and 67[17] of Chapter XI ("Offences"). The provisions were broad in scope and encompassed typical cyber crimes without specificities, a possible explanation for 175 out of the 190 cases in total being booked under Section 66 and 67 of the IT Act, 2000.[18] With the introduction of new offences under the Amendment Act, there are a host of differentiated offences that have criminal penalties attached to them. The new offences range from sending of offensive messages, hardware and password theft to voyeurism, pornography and cyber terrorism, which have been inserted through amendments to Section 66 and 67 of the IT Act, 2000 and form the focus of this paper. In addition, the civil wrongs set out under S.43 of the IT Act have now been qualified as criminal offences under the ITAA 2008, if committed dishonestly or fraudulently.[19]

---

15 Section 65 deals with 'Tampering with computer source documents'.

16 Section 66 deals with 'Hacking with Computer Systems'.

17 Section 67 deals with 'Publishing of Obscene Information'.

18 National Crime Records Bureau, Cyber Crime Statistics (2007), http://ncrb.nic.in/cii2007/cii-2007/CHAP18.pdf.

19 Section 66, IT (Amendment) Act, 2008.

B. Critical analysis of the new offences introduced by the Amendment Act

(i) Sending of Offensive Messages (S.66A)

The introduction of S.66A[20] to the IT Act, 2000 unarguably expands the scope of the act to deal with instances of cyber stalking, threat mails, spam and phishing mails, with an attempt to strengthen the law and circumscribe aspects of unlawful cyber conduct that were left untouched under the old legislation, but a few flagrant issues do emerge on closer inspection of the provision.

The wording in this section has an element of ambiguity in the phrase '*menacing character*', which though perceptibly intended to protect against instances of threat mails or cyber stalking, is too broadly articulated to serve as an effective tool to combat the said offence. While the term '*grossly offensive*' does find mention in similarly purposed legislations, the word '*menacing character*' is conspicuously absent from statutes used by governments to combat instances of cyber stalking and threat mails,[21] which is of assistive value in the assertion that the phrase is misplaced. The expected ineffectiveness of S.66A(a) may be illustrated by the simple example of an employer using a mildly harsh tone in an e-mail correspondence with his employee in order to censure him, declaring possible termination if the employee's indolence continues, or a friend remarking to another in jest, that he will 'beat him up' if he fails to get tickets to the movie they had planned to watch the following weekend. In both cases, one may trace elements of 'menace', so to speak, when it evidently does not exist. Neither does the legislation speak of circumstances where there is reciprocity of sentiments.

---

20 Section 66A: Any person who sends, by means of a computer resource or a communication device,–

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

21 *See*, S.1(a)(i), MALICIOUS COMMUNICATIONS ACT, 1988,(United Kingdom) http://www.harassment-law.co.uk/law/act.htm#, and relevant sections, S.1 and S.4, PROTECTION FROM HARASSMENT ACT, 1997, *available at* http://www.harassment-law.co.uk/law/act.htm#, and CRIMINAL CODE (STALKING) AMENDMENT ACT, 1999, (Australia) *available at* www.legislation.qld.gov.au/LEGISLTN/ACTS/1999/99AC018.pdf.

The fundamental problem with the section, moving on to clauses (b) and (c), is simply that several of the words used in the section such as '*inconvenience*', '*annoyance*', '*obstruction*' or '*ill will*' are not defined either in the primary or Amendment Act, leading to uncertainty in interpretation and increasing the possibility of misuse of the provision, a possible reason for some statutes drafting defences to the charge, within the section itself.[22] However, the efforts of the legislature to address developing situations of cyber crime such as threat mails, e-mail and SMS spamming, cyber stalking and phishing, must be commended.

(ii) Theft of Computer Resource (S.66B)

The relevant section to be analysed in this regard is S.66B[23] of the Amendment Act, which appears to deal with situations where there has been theft of a '*computer resource*' or '*communication device*'. Under this section, an individual who receives a stolen computer, cellphone or any other electronic device fitting the definitions contained within the Act maybe imprisoned for up to three years. Using this section, the police may tackle the growing menace of trading and purchase of stolen laptops and mobile phones, with the caveat of a potentially adverse result ensuing wherein purchasers of second hand phones may be considered suspects or wrongfully charged under this section.[24]

There may be an allegation of redundancy of this section given the pre-existence of a criminal provision for '*dishonestly receiving stolen property*' [25] with identical phraseology and punishment, but such an accusation may be displaced if one exercises scrutiny over the relevant definitions. '*Computer resource*' has been defined to include '*data*',[26] thus markedly different from the IPC provision,

---

22 Title 47, Section 223(e), COMMUNICATIONS DECENCY ACT, 1997 (United States of America), *available at* http://www.cybertelecom.org/cda/47usc223.htm..

23 Section 66B: Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

24 Naavi, *Is ITA 2000 Stringent Enough on Cyber Criminals?*, NAAVI.ORG PORTAL ON INDIAN CYBER LAW (February, 2009), http://www.naavi.org/cleditorial09/editjan27itaaanalysis12deterrance.htm (last visited December 12, 2009).

25 Section 411, INDIAN PENAL CODE, 1860: Whoever dishonestly receives or retains any stolen property, knowing or having reason to believe the same to be stolen property, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

26 Section 2(1)(k), INFORMATION TECHNOLOGY ACT, 2000: "computer resource" means computer, computer system, computer network, data, computer data base or software.

the significant implication being that an electronic document, CD or text message containing stolen information may be brought within the umbrella of '*computer resource*'. In terms of technological significance, this can be extended to include theft of digital signals of TV transmissions.[27]

Interestingly and more importantly, one finds that this section is in consonance with the statements of objects and reasons of the IT Act, 2000 and ITAA, 2008 as it stresses on the need to protect e-commerce and e-transactions involving informational exchange and electronic data exchange.[28] With the introduction of S.66B, and the criminalisation of stolen information transmission and retention, there is a crucial deterrent factor attached to illegitimate or illegal data exchanges which is the primary focus of the IT Act itself. The immediate focus of the Amendment Act, *inter alia*, is the prevention of cyber and computer crimes and utilising the framework laid down previously in this paper and the identification of unlawful cyberspace conduct, it is also known that offences against the availability of computer data and systems (including the 'misuse of devices' with respect to sale, procurement, import and distribution) must be criminalised[29] and the section succeeds in doing so.

(iii) Identity Theft and Impersonation (S. 66C and S. 66D)

An examination of identity theft protection laws for internet users indicates that the harm sought to be prevented is not radically different from the territorial crime of the same nature. The basic nature of the crime involves the use of identifying information of someone to represent oneself as the individual for fraudulent purposes, essentially, the wrongful appropriation of one's identity by another.[30] While familiar traditional crimes of identity theft would include forgeries featuring credit cards, thefts and making of false statements, online

---

27 Naavi, *Information Technology Act 2000 Amendment Details unveiled*, NAAVI.ORG PORTAL ON INDIAN CYBER LAW (December, 2008), http://www.naavi.org/cleditorial08/editdec25itaaanalysis1.htm (last visited December 12, 2009).

28 Statement of Objects and Reasons of the Information Technology Act, 2000, *available at* http://naavi.org/ita2008/objects2008.htm and Statement of Objects and Reasons of the Information Technology Amendment Act, 2006, *available at* http://naavi.org/ita_2008/index.htm (last visited December 12, 2009).

29 *Supra* note 11.

30 Neal K. Katyal, *Criminal Law in Cyberspace*, 149 (4) U. PA. L. REV. 1027 (2001).

versions of the same crime merely involve the use of computers with similar consequences, for example, logging into someone's account and making a defamatory statement, online shopping using someone else's credit card etc.

Prior to the amendment act, the crime of identity theft was forcibly brought under S.66 within the ambit of 'hacking',[31] which presupposes that there was an infiltration of a computer resource involving '*alteration, deletion or destruction*' of the information residing therein, facilitating the crime of identity theft. However, under the new provision, S.66C,[32] the means by which the identifying information is accessed is discounted and only the act of making fraudulent or dishonest use of the information itself is criminalised. The benefit of separating the two offences cannot be overemphasised, given that a separate criminal provision exists for extraction of such data through fraudulent means.[33]

While S.66C deals with deceitful use of passwords, electronic signatures and the like, S.66D[34] involves use of a '*communication device*' or '*computer resource*' as a means of impersonation, which in effect, entails the use of computers, cellphones and PDA's for fraudulent purposes. While the former provision includes intangible but unique identifiers and symbols attached to individuals, the latter envisages instances where the offender has physical access to someone else's personal devices. However, in the absence of a clear definition of '*unique identification feature*' and the advent of new forms of cyber crime such as SMS spoofing,[35] there may exist grey areas relating to identity theft, such as the misuse of cellphone numbers, which, in the strict sense, may not be consistent with

---

31 Section 66, IT Act, 2000: (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

32 Section 66C, ITAA, 2008: Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

33 Section 43 under the IT Act imposes civil penalties for such acts, but after notification of the IT (Amendment) Act, 2008, under Section 66, it is a criminal offence if *mens rea* exists.

34 Section 66D: Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

35 *See* Vineeta Pandey, *Cell Abuse: SMS Spoofing's Forgery*, The Times of India, July 18, 2004, http://timesofindia.indiatimes.com/india/Cell-abuse-SMS-spoofings-forgery/articleshow/782197.cms (last visited December 16, 2009).

the idea of a '*unique*' identification feature of an individual, and not fitting the definition of 'computer resource' or 'communication device' under S.2(1)(k) and (ha), may lie outside the scope of both, S.66C and S.66D, which is a serious concern for cyber crime officials.

A comparative analysis of the punishment stipulated under these provisions with identity theft provisions of other jurisdictions may be attempted to critically examine the nature of punishment under the Amendment Act. One must acknowledge the fact that similar legislations have different degrees of punishment based on the nature of crime committed subsequent to the identity theft taking place, a provision that could have been transplanted into the Indian legislation to make it more comprehensive, instead of having a uniform punishment of three years for the crime of identity theft.[36] So, for example, if the crime involves drug trafficking, or is a violent crime, the punishment is lesser[37] than if the offence is committed to facilitate an act of domestic terrorism.[38] It may also depend on the value of goods or money accumulated over a period of time as a result of the identity theft[39] and may also vary based on the number of identifying markers stolen.[40]

(iv) Voyeurism (S. 66E)

Based on the theoretical framework laid down earlier, the offence of voyeurism would locate itself under the heading 'content-related offences' and based on the subject of the crime, may be slotted into the category of crimes against individuals, specifically, against their person. While the Expert Committee's Report made a recommendation for imprisonment for a period of one year and fine not exceeding rupees two lakh,[41] the Amendment Act

---

36 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028 112 Stat. 3007 (1998).

37 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b)(3)(A) 112 Stat. 3007 (1998).

38 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b)(4) 112 Stat. 3007 (1998).

39 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028 (b)(1)(D) 112 Stat. 3007 (1998).

40 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b) 112 Stat. 3007 (1998).

41 Ministry of Information Technology, Report of the Expert Committee, http://www.mit.gov.in/download/ITAct.doc (last visited December 16, 2009).

prescribes imprisonment for a period of three years but similar fine of rupees two lakh. However, it does not make mention of compensation to the victim which was explicitly recommended by the Expert Committee, to the tune of rupees twenty five lakhs.[42]

The issue that immediately springs up on an analysis of the provision is whether it is appropriate to refer to the wrongful conduct represented in the section as 'voyeurism' in the literal sense since 'observation' of the 'private area' of persons is not criminalised. While this is understandable if one assumes the circumstances under which the offence was introduced in the Bill[43] as not requiring such a provision, since it was not observation as such, which was the concern at the time, but rather, capturing, transmitting and publishing the image of private parts of an individual.

However, on glossing over the Standing Committee's Report, it is clear that it acknowledges the emergence of new forms of computer misuse and is concerned with situations of '*video voyeurism*'.[44] Based on these considerations, it is absurd to exclude from the purview of the section, the 'observation' of private areas of a person. To reinforce this assertion, we may divert our attention to similar criminal legislations, which do include 'observation' within the section, such the Sexual Offences Act, 2003 of the United Kingdom[45] and the Canada Criminal Code.[46] It is also relevant to note that these statutes include viewing of 'private acts' besides 'private areas' of persons, which has been ignored in the Amendment Act. Finally, the observation that may be made, taking into account cyberlaw jurisprudence and the nature of acts that the IT Act seeks to criminalise, is that viewing of such images or videos through online streaming on a website such as YouTube or downloading and viewing on a communication device or computer resource as defined under the Act should also have been specified as illegal within this particular section.

---

42 *Id.*

43 One of the main circumstances for the introduction of this provision was the DPS MMS scandal. The scandal involved a video clip featuring two students from Delhi Public School, one of whom recorded the video on his cellphone, distributed it to his friends, which was further forward to the others, eventually finding its way on to the internet and being listed for sale online. The episode resulted in criminal proceedings being launched against the CEO of Baazee.com. See Avnish Bajaj v. State, 2008 150 D.L.T. 769.

44 Ministry of Information Technology, Report of the Standing Committee (2006), ¶¶ 3 and 6, *available at* http://www.naavi.org/cleditorial07/standingCommitteereportita2006.pdf (last visited December 16, 2009).

(v) Cyber Terrorism (S.66F)

Perhaps the most contentious issue in relation to the Amendment Act is that of cyber terrorism, which is essentially the convergence of terrorism and cyberspace.[47] Terrorism, by itself is not a new phenomenon, but with the development of modern technologies, the creation of laws specifically dealing with the same or related acts, conducted through the medium of cyberspace, was imminent.

An analysis of this section can be fractioned into the first and second clause, the subject matter of each being considerably dissimilar with their own particular complications. The section is comprehensive in that sub-clause (A) first enumerates the methods by which the act is committed, the wrongful conduct, as it were,[48] and then proceeds to describe the potential damage that may be caused by such acts. However, in the portion describing the likely damage, the definition is restricted to cases linked to destruction of property or death of individuals.[49] While the clause also speaks of damage to essential supplies and critical information infrastructure, there is no mention of damage to private property. Using the generally accepted definition of cyber terrorism,[50] it is clear that damage need not be restricted to property belonging to the government. So long as it induces fear in the minds of people, it may be regarded as terrorism. Also, being a provision specific to cyber terrorism, it is surprising that the term

---

45 Section 67(1): A person commits an offence if— (a) for the purpose of obtaining sexual gratification, he observes another person doing a private act, and (b) he knows that the other person does not consent to being observed for his sexual gratification....

46 Section 162(1): Every one commits an offence who, surreptitiously, observes — including by mechanical or electronic means — or makes a visual recording of a person who is in circumstances that give rise to a reasonable expectation of privacy....

47 *Supra* note 9, at 62.

48 *See* Section 66F 1(A) (i), (ii) and (iii).

49 Section 66F 1(A):...and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure....

50 'Unlawful attacks against computers, networks and the information stored therein, when done to intimidate or coerce a government or its people in furtherance of political or social objective', Peter Grabosky & Michael Stohl, *Cyberterrorism*, 82 REFORM 8 (Autumn, 2003).

'virtual properties',[51] belonging to both the government or private citizens, has not been used anywhere in the section.[52]

In the second sub-clause,[53] predominantly dealing with access to sensitive information, data and computer databases (possibly belonging to the military), there is no explicit mention of specific cyber-related activities or offences, which may have provided additional clarity as to the manner in which the penetrated data or information may be used to imperil the security of the State. For example, the data may be used to locate sensitive targets, private bank accounts may be used to fund terrorist programmes and terrorist propaganda may involve dissemination of confidential data divulging military capabilities of the State in question. It is obligatory for the definition to cover acts involving the internet such as money settlement through internet banking, use of internet channels to communicate terrorist plans across countries, hacking and defacement of governmental and non-governmental websites, virus and trojan attacks aimed at secure infrastructural and cyber assets of the country etc.[54] What is undesirable is to have an overlap of functional definitions between the IT Act, the IPC and the Unlawful Activities Prevention Act as this will only create ambiguities and loopholes that will aid the terrorists eventually. Thus, the section does not seem comprehensive enough to cover most unlawful conduct on the internet that would typically be associated with cyber terrorism.

In an effort to analyse and contrast this section with similar criminal provisions across territorial jurisdictions, we may divert our attention to the issue of punishment prescribed under the section and whether the section is devised in a manner that exhibits recognition of international developments

---

51 Virtual property may include accounts, websites, virtual currency, virtual housing spaces and other real estate in cyberspace, virtual pets, weapons and characters etc.

52 *See* Naavi, *ITA 2000 Amendment Bill defines Cyber Terrorism, prescribes life sentence*, BLOGGER NEWS NETWORK (December, 2008), http://www.bloggernews.net/119157 (last visited December 10, 2009).

53 Section 66F 1(B):...knowingly or intentionally penetrates or accesses a computer resource without authorisation... any restricted information, data or computer database... so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State....

54 Naavi, *IT Acts Amendments and Cyber Terrorism*, MERI NEWS (December, 2008), http://www.merinews.com/article/it-act-amendments-and-cyber-terrorism/152449.shtml (last visited December 8, 2009).

in cyber crime, especially in relation to cyber terrorism. Considering the content of the law, there does not appear to be widespread discrepancies with cyber terrorism-centred legislations across the world taking cognisance of the fact that there is an increasing use of computers to facilitate attacks of terrorism,[55] and that 'it is safer and more convenient to conduct disruptive activities from a remote location over the Internet than it is driving planes into buildings'.[56] As regards penalties, imprisonment for life appears to be the norm across jurisdictions[57] and uniformly the harshest amongst all internet-related crimes.[58]

It is inconceivable to think that the cyber terrorism provision in the IT Act will lie stagnant in the years to come, given the dynamic nature of terrorist activity, which is bound to traverse yet unforeseen criminal territories, but it is discomforting to see that the first legislation addressing the incidence of cyber terrorism falls drastically short in terms of comprehensiveness, clarity and particularity.

(vi) Sexually Explicit Content and Child Pornography (S.67A and S.67B)

Without entering into complicated questions of internet content regulation and obscenity on the internet, an analysis strictly of the provisions of the amendment Act reveals the section dealing with sexually explicit content, S.67A, a sub-section of S.67, which was present prior to the Amendment Act, to be well drafted and clearly defined. The terms used in the section such as 'publishes', 'transmits' have been previously defined in the act, assisting interpretation of the section to a considerable extent. In terms of penalties, compared to S.67, S.67A has an enhanced imprisonment term as well as fine for both first and subsequent convictions. Since the offence of obscenity is not a new addition to the list of offences, it has been excluded from the scope of this paper.

---

55 *E.g.*, in Australia, § 100.2(2)(h) and (i) of the Criminal Code Act (Cth), include the term '*electronic communication*', to stress on the increasing use of computers as a medium in terrorist activities. The Criminal Code Act was amended by the Security Legislation Amendment (Terrorism) Act, 2002.

56 Yee F. Lim, CYBERSPACE LAW: COMMENTARIES AND MATERIALS 353 (2007).

57 *See* Section 66F(2) of the IT (Amendment) Act, 2008 and Section 101.1(1) Criminal Code Act (Cth).

58 *Supra* note 56, at 355.

On the matter of child pornography, S.67B is a welcome introduction to the list of offences under the IT Act, particularly for the stringency that has been embedded into the provision, with not only 'publishing' or 'transmitting' of pornographic content involving children, constituting offences, but so also its collection, online viewing, downloading, promotion, exchange and distribution. This is in contrast to the offence of voyeurism as operationally defined under this Act, and previously discussed in this paper, which does not criminalise the act of viewing itself. The problem with the section however, is definitional, with ambiguity in the meaning of the phrase '*abusing children online*',[59] when read along with S.67B(e) which also discusses abuse in relation to children, but specifically mentions the phrase '*sexually explicit*' to indicate the nature of abuse. The absence of the same in the previous sub-clause leads on to believe that the constitution of 'abuse' under S.67(d) is not of a sexual nature, although it is not necessary that they must be mutually exclusive. Further, the use of the word '*indecent*' in S.67B(b) appears problematic when read in conjunction with the word '*obscene*' placed before it in the same sub-clause given that in India, there are obscenity tests laid down through precedent,[60] but nowhere has the word '*indecent*' been defined or explained.

C. The Void for Vagueness Doctrine

In order to support the view that an absence of clarity in criminal statutes is indeed a ground for protest, the researcher would like to briefly examine the Doctrine of Void for Vagueness, indigenous to the American legal system, having been derived from the due process clauses of the Fifth and Fourteenth Amendments to the U.S. Constitution.[61] The basis of the doctrine is uncertainty and lack of specificity and the philosophy underlying the principle appears to be quite simple - no one may be required at peril of life, liberty, or property to speculate as to the meaning of a penal law.[62] Thus, if it is found that a reasonably prudent man is unable to determine by himself the nature of the punishment,

---

59 Section 67B(d) of the Information Technology Act, 2008.

60 *See* Rahul Matthan, *Obscenity and Pornography on the Internet*, in THE LAW RELATING TO COMPUTERS AND THE INTERNET 45 (2000).

61 *Void for Vagueness Doctrine*, LAW.JRANK.ORG, http://law.jrank.org/pages/11152/Void-Vagueness-Doctrine.html (last visited on April 24, 2011).

62 *Id.*

the prohibited conduct as envisaged under the statute, and what class of persons the law seeks to regulate, for lack of definiteness, the law may be regarded as 'void for vagueness'.[63] The objective of a criminal statute is fairly simple, allowing citizens to organise the affairs of their lives with the knowledge of acts that are forbidden by the law, and the negation of this should logically be considered an infirmity of the legal system.

The researcher has used the example of this doctrine to buttress the argument that a criminal statute must be drafted with precision, leaving no room for ambiguity, particularly with reference to phrases that enumerate classes of persons, acts constituting an offence or a generic term that may be susceptible to multiple interpretations. Thus, for example, the phrase 'gangster' when used in a penal statute, may render the statute void, since the phrase is open to wide-ranging interpretations, both by the court and the enforcing agencies.[64]

While there exist several such instances, the author would like to limit the illustrations to this one specific case, merely to demonstrate the fact that mere uncertainty in a single phrase of a hastily drafted statute could render the law unconstitutional and void, thereby necessitating precaution in the framing of penal statutes that are bound to affect a majority of citizens, as is certainly the case with a statute regulating activities on the internet in a country as large as ours.

IV. CONCLUSION

The Information Technology (Amendment) Act, 2008 serves as a suitable case study for an analysis of the legislative exercise of law and policy formulation in the field of cyber crime legislation, revealing quite emphatically the need for carefully worded provisions, foresight in the drafting process and imagination with respect to explanations to particular sections. The inadequacies of the legislation and the resultant realistically anticipated problems reinforce the notion that criminal legislations cannot be left open to broad interpretations, especially with regard to internet regulations, considering the fact that cyberspace provides

---

63 A. G. A., *The Void for Vagueness Doctrine in the Supreme Court*, 109(1) U. Pa. L. Rev. 67 (1960).

64 Lanzetta v. New Jersey, 306 U.S. 451 (1939); Edelman v. California, 344 U.S. 357 (1953).

certain liberties in action that make it easier to transgress laws, and with such characteristics inherent to the environment, any regulatory mechanism or legislative measure must seek to be comprehensive, clear and narrow in interpretive scope.

While the purpose of the Information Technology (Amendment) Act was to address increasing trends of cyber crime and in effect, make it difficult to be a cyber criminal, the irony rests in the fact that what the Amendment Act eventually has created is a situation wherein it perhaps, isn't '*easier to be a criminal*', but rather, '*easier to be classified as a criminal*'. The danger, in both cases, cannot be overemphasised.