Internet Safety & Cyber Law's in India

Advocate Prashant Mali - M.Sc.(Computer Science),LLB,LLM
Cyber Law & Cyber Security Expert

Internet safety is the knowledge of maximizing the user's personal safety and security risks on private information and property associated with using the internet, and the self-protection from computer crime in general[1]. The definition makes it clear that safe guard protection & remedies for human being and their property both are required, In many cases people are not aware about remedies available to them under law when safety of their good self, children or property is compromised. This paper aims at analysing various laws i.e traditional and new laws which protects Internet safety in India.

Internet Safety Laws against Online Obscenity

Whenever a scholar writes a paper on Internet safety in India he or she has to start first with online obscenity which has become plague in India. Obscenity may be verbal or scenic, personal or political, gender biased or unbiased. Internet has become a potent media to vent out all the obscenity in the minds of oppressed Indians shielded by their Hippocratic cultural beliefs. It would right to say in India "There is loads of sex in the minds of people then in the bed" this often finds its way in the form of obscenity on the Internet platform. This is mainly because internet hides people from facial confrontation and gives them sense of false security that they can get away with any misdemeanours and simultaneously derive filthy pleasures.

Section 292 of the Indian Penal Code (IPC) defines obscenity as that which is 'lascivious or appeals to the prurient interest or tends to deprave or corrupt persons'.
In recent supreme court judgement *Aveek Sarkar & Anr Versus State Of West Bengal & Ors* [2] on obscenity, it was held that nude picture of women in not obscene per se. This judgement overruled the Hecklin[3] test which was used to interpret obscenity by courts till date for deciding cases on obscenity.
The amended IT Act, 2000 also has sections which define and restrict what is 'obscene' on the Internet. In this regards section 67, 'publishing or transmitting obscene material in electronic form', and section 67A, 'publishing or transmitting of material containing a sexually explicit act in electronic form'. The latter was added when the said Act was amended in 2008.
Section 67 finds similarities with Section 292 of the IPC, but punishment under the IT Act are much higher, it is a cognisable offence. Section 292, a first conviction can lead to a prison term of up to two years and a fine of up to two thousand rupees. A second or subsequent conviction carries a prison term of up to five years, and a five thousand rupee fine. Now, analysing section 67, the first conviction can lead to a prison term of up to three years and a fine of up to five lakh rupees. In the event of subsequent convictions, imprisonment can extend up to five years, with a fine of up to ten lakh rupees. Section 67 though was predominantly enacted and defined for online purposes.
Section 67A, on the other hand, is a stricter modern legal provision mainly to address pornography. This is a new category of cybercrime and with higher punishments of up to 10 lakh rupees fine and of imprisonment of up to five years for first convictions and up to seven years for one subsequent act.

1.Wikipedia -http://en.wikipedia.org/wiki/Internet_safety.
2. www.stpl-india.in/SCJFiles/2014_STPL(Web)_72_SC.pdf
3. Regina v. Hicklin, 1868

Section 67B is the explicit safe guard for children i.e pupils below 18 years of against child abuse and pornography. This is also a new category of cybercrime and with higher punishments of up to 10 lakh rupees fine and of imprisonment of up to five years for first convictions and up to seven years for one subsequent act. This section encompasses all kinds of possible violations against the child and is a non-bailable offence. This section is a milestone in Indian law to protect and safeguard children on Internet.

Exceptions stated in all the four above sections are materials that can be proved to be 'justified as being for the public good', extending to art, literature, science and learning. However, given that none of these fields are open for wide and vivid interpretation, thus may be subject to individual conscience. Obscene material as one having 'the tendency to deprave or corrupt' is a phrase that has inherent ambiguity, and its potential for varying interpretations may lead, and has led, to disagreements between judges. For example, in the *Aveek Sarkar case,* High Court judge believed the content to be obscene by applying Hecklin Test , whereas the Supreme Court judges overruled the decision, applying it the "Community Standards test" . With no scientific or sociologically accepted definition of what is depraved or corrupting – or, for that matter, a singular understanding and approach to the field of 'art' – a large breadth of interpretative space is created as per the personal values, views and perspectives of individuals.

Interestingly, the definition of obscenity as lascivious (lustful, with a desire for sexual practices) or appealing to the prurient interest (arising from indulgence in lustful thought) is, a concept of obscenity that derives from 19th Century Christianity, 'according to which anything to do with sex is dirty and obscene'. More specifically, the definition of obscenity as provided in Section 292 of the IPC was taken from an English case in 1868, in which the presiding judge declared, when asked to determine whether or not the content of a specific text was obscene,

I think the test of obscenity is this: whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.[4]

With the *Aveek Sarkar case* setting the precedent*, the* Station House Officer (SHO) or In-charge of the police station who registers a police complaint of obscenity suddenly becomes a quasi-judge who would determine whether the photo or matter is obscene and whether is depraving the mind of common man even if the photo exhibits full or partial nudity.

In the IT Act, Section 66E of the IT Act concerns 'punishment for violation of privacy' and reads: Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

The other Act namely Indecent Representation of Women (Prohibition) Act, 1986 (IRWA), The Act defines the 'indecent representation of women' as a

publication or distribution in any manner, of any material depicting a woman as a sexual object or which is lascivious or appeals to the prurient interests; or depiction, publication or distribution in any manner, of the figure of a woman, her form or body or any part thereof in such a way as to have the effect of being indecent or derogatory to or denigrating women or which is likely to deprave, corrupt or injure the public morality or morals.

2. Quoted in Mazzarella, William (2011).

Internet Safety Laws against Online Verbal Abuse

Even though it is said “A Picture is worth a Thousand Words” in the age of internet where picture files are heavier in size than words, written words tend to spread faster than what even the writer thinks it would spread. Whispers in real world take more time to spread than a casual comment written online spreads. facebook, twitter, blogs, emails, WhatsApp are new age media used for the same. *Shaheen Dada Case* of her mentioning a status on facebook and the chronology of events thereafter created a furore in the country. Again here it lies with the conscience of the police manning the complaint table to appreciate what the complainant brings on table is grossly offensive or having menacing character. Imagine the ordeal of junior level officer who probably never feels anything obscene when he is hurled abuses by his seniors or politician masters. Now s/he is to judge “is it grossly offensive ?” what complainant says he or she is indicted upon via Internet.

Section 66A – The saviour from online defamation or abuse

For people seeking recourse to the law to fight online defamation or abuse, section 66A of the IT Act, 2000 would be the best option to register a case under, as it is comprehensive in the wordings and can be widely interpreted and applied. The section was included wide amendment of 2008, and deals with the sending of offensive messages through communication services. It is also an anti-spam law of India. The section reads:

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; or

(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.

This section of the IT Act, 2000 is “substantially the same” as laws instituted in other democracies like UK and the United States. What’s more, the language that is employed in various sections is exactly the same.

In *Manoj Oswal v State of Maharashtra*[5] Bombay High Court decision gives Section 66A a much wider scope than was previously thought, the High Court pointed out that interpreting Section 66A to include websites within its purview. By interpreting the term 'send' to mean the same as 'publish or transmit' the Court has widened the scope of Section 66A. This interpretation of Section 66A makes redundant Sections 499 and 500 of IPC which punishes any false imputation that is published and harms a person's reputation, provides the defence of justification by truth and cannot be used to harass the innocent since it is non - cognizable and bailable.

Furthermore, offences under section 66A are cognisable, which means if the investigating officer in the matter feels the information at hand is Grossly offensive or having menacing character, he can arrest the accused without warrant. In addition to this, sub-section (c) of 66A states that the law can be applied to ‘electronic mail messages’, which in effect includes mobile phone SMS & WhatsApp messages that may serve to ‘annoy’ or ‘inconvenience’ someone.

5. Criminal Writ Petition No. 314 of 2012

Even though incident of Mumbai resident Shaheen Dhada facebook status update matter or a man with less than 16 followers on Twitter was arrested under the same section for alleging that the son of Indian Finance Minister P. Chidambaram was corrupt or the Mamata Banerjee's matter with the journalist have time and again raise heckles from supporters of free speech, this section remains savour for whom once they are defamed or abused online. I feel there can be no substitute words for "Grossly Offensive" or "Having Menacing Character" as of date which describes the ordeal of an individually harassed online to the brink of his life. The only notable changes to this section are the Investigating Officer needs to take permission from a officer of the rank of DCP or DIG before making any physical arrests in the matter.

The IPC contains various sections that address crimes of verbal abuse against and the harassment of a lady section 354A added by the Criminal Law (Amendment) Act 2013, this is more comprehensive definition of sexual harassment, than initially provided under section 509 of the IPC and which includes the following acts:
(i) physical contact and advances involving unwelcome and explicit sexual overtures; or
(ii) a demand or request for sexual favours; or
(iii) showing pornography against the will of a woman; or
(iv) making sexually coloured remarks.
Cyber Stalking which was effectively missing in The IT Act,2000 is covered in the IPC under Section 354D via amendment of 2013 explicitly includes crimes that involve *monitoring the electronic communication of a woman*. The section reads:
Any man who –
(i) follows a woman and contacts, or attempts to contact such woman to foster personal interaction repeatedly, despite a clear indication of disinterest by such woman; or
(ii) monitors the use by a woman of the internet, email or any other form of electronic communication; commits the offence of stalking
Section 507 of the IPC – criminal intimidation by anonymous communication – is a different provision that may be used by people facing harassment and threats online, particularly given the fact that extortion, blackmail & rape threats are the most common form of verbal harassment faced by any individual. To qualify compliant for this section there has to be clear criminal intimidation as defined under 503 of IPC.
Another relevant section of the IPC that may be used along with section 66A of the IT Act, 2000 is section 499, which pertains to defamation. The section reads:
Whoever, by words either spoken or intended to be read, or by signs or by visible representations, makes or publishes any imputation concerning any person intending to harm, or knowing or having reason to believe that such imputation will harm, the reputation of such person, is said, except in the cases hereinafter expected, to defame that person.

The Internet related abuse and defamation has had a massive impact on many areas of personal and professional life. While defamation, in the shape of slanderous and libelous comments, has been around for many decades, the problem has been exacerbated by the advance of the Internet as a reporting and social tool. While comments made in newspapers and even on the TV have a limited shelf life, those made on the Internet can remain on the website where they were first added as well as on other blogs and websites and even in the cache of search engines for many more years. Hence the knowledge of law & remedies plays an important role.

Internet Safety Laws against Online frauds (Banking and Non-Banking)

The Indian banking and financial services sector has witnessed exponential growth in the last decade. The growth has not been without its pitfalls as incidents of frauds in the industry have also been on the rise[6]. Beginning 2014, I have lodged cases of online frauds worth more than 2.5 crore in various legal forums. Even though penetration of ecommerce and usage of internet banking has increased, the safety related knowledge but knowledge related to remedies under law is yet to sink in with the common man using Internet for commercial activities.

Various laws covering frauds are Indian Penal Code (IPC), the Information Technology Act, 2000 ,Special Enactments – i.e., Prevention of Money Laundering Act, 2002; Prize Chits & Money Circulation Schemes (Banning Act, 1978) and its yet to come in force draft Money Circulation Scheme (Banning) Rules, 2012, Indian Contract Act, 1872,

S.17 Indian Contract Act, 1872: `Fraud' includes acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract:- (1) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true; (2) the active concealment of a fact by one having knowledge or belief of the fact; (3) a promise made without any intention of performing it; (4) any other act fitted to deceive; (5) any such act or omission as the law specially declares to be fraudulent. Explanation -Mere silence as to facts likely to affect the willingness of a person to enter into a contract is not fraud, unless the circumstances of the case are such that, regard being had to them, it is the duty of the person keeping silence to speak, or unless his silence, is, in itself, equivalent to speech.
No definition of fraud is given in IPC. Most acts done with "dishonest" or "fraudulent" intent however are classified as criminal offences, like: Cheating (417 – 420 IPC); Misappropriation and criminal breach of trust.(403; 405);Forgery including of electronic records including with intention to cheat; harm persons' reputation; by employee etc.,; (463 – 471 IPC);IT Act – S.43 r/w S.66; S.66C; 66D;

Once a person is a prey of any Internet or online fraud and he wants to lodge a criminal complaint, he can do so in the nearest police station of his jurisdiction or at the cybercrime police station. VICTIM needs to file the case under Section 66C & 66D of The IT Act, 2000 and if hacking is also involved Section 66 also can be applied. Sections 420,471,419 of the IPC also can be applied.
The relevant IT Act section mainly applicable are further expanded
S.66C: Identity Theft: Fraudulent or dishonest use of electronic signature, identity password or unique identification feature – punishable with imprisonment up to 3 yrs & fine of up to Rs.1 Lac.; S.66D: Cheating by impersonation –punishable with imprisonment up to 3 yrs & fine of up to Rs.1 Lac.
Section 43(g), Section 43A and Section of 85 can be applied, when filing a complaint against banks, finance or telecom companies for online banking or credit card frauds. This complaint has to be filed with the Hon. Adjudicating officer (a type of cybercrime court) who is appointed under section 46 of The IT Act,2000 and normally sits in Mantralaya or Science & Technology Departments of the state.

---

http://www.deloitte.com/assets/Dcom-India/Local%20Assets/Documents/Thoughtware/India_Banking_Fraud_Survey_2012.pdf

Internet Safety Laws against Property

In Internet domain one has to guard against their identity being stolen, your domain name being taken, the data you own may be under theft, Virus or malicious code being implanted on your computer or your trademarked or copyrighted material is infringed.
The IT Act, 2000 provides two remedies one being criminal and other being civil for providing compensation. The claim for compensation up to Rupees Five crores would lie with the Adjudication Officer appointed under Section 46 of The IT Act, 2000.Now, looking at criminal various actions, Section 43 has to be read with Section 66 which apply for all crimes mentioned in section 43 and envisages punishment with imprisonment for a term which may extend to three years or with fine which may extend to Five lakh rupees or with both .Various sections applicable are as follows:
For Data Theft Section 43(b), For Hacking Section 43(a), For spreading Virus or malicious code Section 43(c),For causing damage to computer or network (vandalism) Section 43(d),For disrupting computer or Network Section 43(e),For Denying access to computer or Network Section 43(f),For helping hackers Section 43(g),For tampering computer or network Section 43(h),For destroying or altering any data Section 43(i) and For stealing, deleting or altering any source code Section 43(j) would apply.
In India, the offence of Copyright infringements are pursued under section 63 of the Copyright Act, 1957 'whereby any person who knowingly infringes or abets it shall be punishable for term not less than 6 months extendable upto 3 years with fine not less than rupees 50,000'.This section is applicable for Software Piracy in cyber space.
Section 65 of The IT Act,2000. Tampering with Computer Source Documents.- Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to 2 lakh rupees, or with both.
Explanation - For the purposes of this section, "Computer Source Code" means the listing of programme, Computer Commands, Design and layout and program analysis of computer resource in any form.

Conclusion

Internet which came as a use full aid to business and education has now fully blown into an entity which has its own existence, its own social aura and tenets. Digital literacy, safety & security comes with dissipated awareness & knowledge of safeguards and laws governing the Internet usage. Laws in India though enacted with full vigour are not implemented with the same *josh*. Common IT user often do not know various sections of laws and there rights under the law, I find difficult to digest that educated people cannot differentiate between civil or criminal remedies available to them under law. I feel Laws hence further enacted should have a section which mandates all states and municipalities to conduct awareness trainings and further the budget for the same should be allocated in the law itself for next ten years. This paper has aimed to make Internet or Online users aware about various Cyber Laws available and remedies under the same and thereby causing general awareness.

Advocate Prashant Mali is a practising lawyer, a renowned Cyber Law Expert and A Cyber Thinker in India. He is a charismatic and hobbyist Author. **Connect:** Facebook.com/cyberlawconsultant **|** ***Email:****cyberlawconsulting@gmail.com* **|Twitr:** *@CyberMahaGuru*