INTERFACE BETWEEN TECHNOLOGY AND SOCIETY: A STUDY OF THE LEGAL ISSUES

Atin Kumar Das[1]

I. Introduction

The increase in the use of technology brings added responsibility to the legal professional. The internet have grown much beyond their traditional computing roles and gained access to all the types of human activities. The real world legal system functions on the basis of certain established assumptions that may not be applicable to the virtual world. So we have very clear as to the differences between these two worlds in order to understand the issues and difficulties in establishing real world legal control over the virtual world.

II. Technology and Vulnerability

Information technology and internet in particular offer some new and highly sophisticated opportunities for law breaking, and they create potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerised systems for almost everything in life, from train to medical service condition and national security. Society's dependence on computer systems, therefore, has a profound human dimension. Destructive acts using computer networks have cost billions of dollars and increasingly threaten the resources of network connected critical infrastructures.[2]

III. Real World and Virtual World

Real world is a physical entity, with well defined borders dividing it into sovereign states. It functions on the basis of sovereignty of the nation states over its territory and inhabitants.

The virtual world confirm to none of the accepted requirements of the sovereignty. Cyberspace does not have a permanent population, it definitely has no territory, it has no government, and it has no capacity to enter into diplomatic relations. Therefore, the very concept of sovereignty is

---

[1] Assistant Professor in Law, Haldia Law College, ICARE Complex, Hatiberia, 721657, Purba Medinipur, West Bengal

[2] S.V. Jaga Rao, *"Computers Contracts & Information Technology Law"*, P.29. (Nagpur: Wadhwa & Co., 2003): It is the rule of nature that there can be nothing perfect. True to this rule of the nature, the information technology also has its negative side. It has opened up the windows of opportunity to anti socials and criminal too, to expand their nefarious activities to the cyber world.

not amenable to the virtual world called cyberspace. Persons enter the digital world by going online and come out of it by merely disconnecting. No one is a permanent member there and any one can enter it at a given time provided has access to it through connectivity. It has no centralised authority controlling its affairs. Even the largest regulatory body in the internet, ICANN, has a very limited role of allocating and regulating domain names and no other control over the activities of the net. These fundamental differences from the real world make cyberspace not an easy entity to regulate, because the real world regulations functions, as already mentioned, on the basis of certain established assumptions.[3]

IV. Issues of Jurisdiction

The issues of jurisdiction is the main barrier from the technology and legal challenge because the offender might sitting in one country and using a system situated in another country might commit a crime in a third country.[4] The legal responses in each of these countries could vary and the jurisdiction of one particular country may depend on the legal system that is followed therein. Even when a particular country assumes jurisdiction and set out to prosecute the offender, issues like investigation, evidence, trial (lex loci and lex fori) poses problems.[5]

The main solution of this problem is divided by the researcher in two ways:

i. The enforcement measure is not territorial but global.

ii. The nations must co-operate and co-ordinate in their activity in regulating the cyber space.

---

[3] Pavan Duggal, *"Cyber Law"*, P.8. (New Delhi: Universal Law Publishing House, 2014): In India context, in the beginning, the Internet – related disputes that emerged were the domain name disputes. A lot of these disputes arose prior to the coming into effect of the Uniform Domain Name Disputes Resolution Policy of the Internet Corporation For Assigned Names and Numbers (ICANN).

[4] Rahul Matthan, "*The Law Relating to Computers and the Internet*".P.25, (New Delhi: Butterworths Publications, 2004.)

[5] Rodney D. Ryder, "*Guide to Cyber Laws,"*P.369, (Nagpur: Wadhwa Publications Ltd, 2002): The offender might by sitting in one country and using a system situated in another country might commit crime in a third country. Even in such relatively simple situations, number of countries involved may be much more since the transaction was accomplished by information flows through various other countries, without the knowledge of the offender. The legal responses in each of these countries could vary and the jurisdiction of one particular country may depend on the legal system that is followed therein.

V. Children and Internet

The growing access and use of IT by children also increases their exposure to potential risks of online abuse and exploitation. Cyber offences against children are spreading and diversifying as new methods are used to harass abuse and exploit children. In many instances, children are also online offenders. Offline forms of crime and violence against children are finding new forms of expression in the online violence are interrelated, since online abuses also include offline components sometimes.

Table 1: Current forms of child online abuse and exploitation include:[6]

Cyber Bullying	Emotional harassment, defamation and social exposure, intimidation, social exclusion.
Online Sexual abuse	Distribution of sexually explicit and violent content, sexual harassment.
Online Sexual Exploitation	Production, distribution and use of Child sexual abuse material, child pornography.

There are no reliable figures on the extent, patterns and trends of child online abuse and exploitation in India, since no comprehensive surveys have been carried out on these issues.

Table 2: Indian Laws/Policies to safeguards children online[7]

Law/Policy	Provision	Punishment
The Information Technology Law, 2008	The newly inserted Section 67B by an amendment of 2008 in the IT Act, 2000 attempts to safeguards the privacy of children below 18 years by creating a new enhanced penalty for criminal who target children.	Imprisonment upto five years (seven) years for repeat offenders and with a fine of upto Rs. 10 Lakhs.
Criminal Law Amendment Act, 2013/Indian Penal Code, 1860	As the Information Technology Act, does not have specific provisions for criminal intimidation, hate speech and defamatory content, the provisions of the IPC apply in Online offences.	Nil

[6] Types of Child Sexual Abuse, NSPCC (Source): http://www.nspcc.org/child-sexual-abuse. (Last Visited on: 04/12/2016).

[7] Pavan Duggal, *"Cyber Law"*, P.227. (New Delhi: Universal Law Publishing Co. 2014).

Protection of Children from sexual offences (POCSO) Act, 2012	Section 12 and 14(2) Which deals with online offences against children, including pornography and grooming.	5 years and in case of subsequent conviction, 7 years.
The National Policy for Children (NPC) 2013	Does not refer directly to online risks. All policies related to education, ICT or cyber security are expected to incorporate the principles of the NPC and provide children with equal opportunities for learning and environment, while protecting them from harm.	Nil
The National Policy of ICT in School, 2012	Is more explicit about regulating ICT to protect from potential risks. It recognizes online risks and has provisions for regulating and monitoring Internet access.	Nil
The National Cyber Security Policy, 2013	Addresses the prevention, investigation and prosecution of cybercrimes, including those against children.	Nil

In addition, the newly draft intermediary Due- Diligence Guidelines, 2011 require 'intermediary' to notify users not to store, update, transmit and store any information that is inter alia, "paedophilic" or "harms minors in any way". An intermediary who obtains knowledge of such information is required to "act expeditiously to work with user or owner of such information to remove access to such information that is claimed to be infringing or to be the subject of infringing activity". Further, the intermediary is required to inform the police about such information and preserve the records for 90 days.

VI. Limitation of laws and Policies

Many activities that have been criminalized in other countries such as cyber bullying, are not regarded as offences by Indian Law. Legal provisions for addressing cyber bullying are lacking. While child trafficking with the intent of sexual exploitations criminalized, but child trafficking

with the intent to produce pornography and advertise child sex tourism online is not.

VII. Invasion into the privacy of Individual

With Information and Communication Revolution pacing fast to broaden its horizon, the Internet has become the fastest growing means of communication through e-mails, chats, browsing, etc. The Internet has changed the structure of the society in a way that the computer today occupies a very important place in our lives.

Our civilisation has progressed through ages breaking all geographical barriers and the most notable addition to the human civilization, in recent years, is the Internet, bringing the whole worlds closer and turning it into a 'global village'. But this 'closet global village', the cyberspace, is now a space with new risks, which challenges the very essence of individual privacy. People's interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology.

The new technologies have enhanced the possibilities of invasion into the privacy of individuals and provided new tools in the hands of eavesdroppers. Individual privacy is at a great stake than ever before. Electronic gadgets and the Internet can be used to amass huge amount of data regarding people, profile it in various ways, commodify it and deal with it in a manner which could violates individual privacy.

Table 3: Indian Laws/Policies to Safeguard Privacy of Individual

Laws	Provisions
Law of Torts	Publicity given to private life: the facts which are so private for which anybody has a reasonable expectation of privacy being maintained, if they are made public, i.e., if they are put on the Internet, then this amount to a common law of tort.
Indian Constitution	In common law, a private action for damages for unlawful intrusion of privacy is maintainable. Under Article 21 of the Indian Constitution must be read together with the constitutional right to publish any matter of public interest, subject to "reasonable restriction".
The Information Technology Act, 2000	The act does not deal with the issue of privacy directly but a few provisions of the statute have bearing on the right to privacy. Section72 of the IT Act entitled "Penalty for breach of Confidentiality and privacy".
The Information Technology	The act prior to the previous Act does not deal with the issue of privacy but a few provisions of the

Amendment Act, 2008	statute have bearing on the right to privacy. Section66E of the IT Act entitle "Punishment for violation of Privacy".
The Criminal Law Amendment Act, 2013	For the first time, the 153 year-old Indian penal code now recognizes the issue of privacy and provide punishment to those who watched, or recorded, without their consent, where the victim could reasonably expect privacy.

Table 4: Human Right Perspectives on Privacy[8]

Human Right Conventions	Provisions
Universal Declaration of Human Rights, 1948	Article12 of UDHR recognize the Privacy of family, home and honour/reputation.
The International Convention on Civil and Political Rights, 1966	Article 17 specifically recognizes privacy as a right.
European Convention for the protection of Human Rights and Fundamental Freedoms 1950	Article 8 everyone has the rights to respect for his private and family life, his home and his correspondence.

It is apparent that the larger issue of online privacy has remained completely outside the scope of the legislation. There seems to be no particular authority concerned with understanding the importance of the issue and bringing in regulations to curb unscrupulous use of personal information. It is not even as if a self regulatory model for online business is in place and legislation is not required. It is important that legislators understand that the protection of personally identifiable information is vital if one seeks to foster a secure and trustworthy electronic environment the avowed purpose of the IT Act. This is one void in law and policy that just cannot be ignored.

VIII. Enforcement Regime

The IT Act, 2008 has been an epoch-making legislation. The eonic approach has laid down a new legal erection for the enforcement department. It will not be wrong to say that this amendment has been cybercrime friendly and paves the way for an effective, result bearing and comparatively simpler way of investigating cybercrimes.[9].

---

[8] UDHR adopted and proclaimed by General Assembly resolution 217A (III) of December 10, 1948, source: http://www.un.org/overview/right.html.(Last Visited on: 04/12/2016).

[9] Talat Fatima, "*Cyber Crimes*", P.440 – 443. (Lucknow: Eastern Book Co. 2011). It also depicts the seriousness of law makers regarding cyber security in the

Table 5: Enforcement Measures

Regarding Cyber Security	Regarding Investigations of Cybercrimes
Critical Information Infrastructure (CII), Section 70(I) defines the term "Critical Information Infrastructure" means the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.	**Section 78** has been amended to replace the word "Deputy Superintendent of police" by the word "Inspector". **Section 80** provides inspector to enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed any offence under this Act.
Protected System, Section 70(I) (Amended) defines the term "Protected System" has been enlarged to bring within its ambit the CII.	**Section 2(ha) "communication device"** means cell phone, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.
National Nodal Agency, Section 70-A, to ensure cyber security in the country there is provision for the establishment of National Nodal Agency.	**Section 79-A** – this newly added section shall also be of a great help to the enforcement department as it is for the first time that a technological expert has been included to aid the legal procedure.[10]
Indian Computer Emergency Response Team (ICERT) According to section 2(iia) of the IT Act, 2000 "Indian Computer Emergency Response Team" means an agency established under sub-section (I) of Section 70-B[11].	**Section 84-B** for the first time makes abetment of offences under the IT Act an offence. According to Section 84-B if anyone is found guilty of abetting an offence under the IT Act no separate punishment is given fr it then he will be punished with the punishment prescribed for the

country and has taken in its stride most of the difficulties and hardships faced by the law-enforcers. The government approach has been two pronged.

[10] Inserted by virtue of S. 40 of the IT (Amendment) Act, 2008 (10 of 2009) and a new chapter XII-A has been added which includes the section 79-A *Central Government to notify Examiner of Electronic Evidence.*

[11] Inserted by S.36 of the IT (Amendment) Act, 2008 (10 of 2009). The central government shall make arrangements for the establishment of a central entity to serve as ICERT. This will be a specialized body primarily to take care of the protected system in the country.

	commission of that offence.[12]
Monitoring, interception and decryption of data- Section 69[13], 69-A[14] and 69-B[15], empowers the government to authorise any agency to take these steps as per the rules prescribed by the government. The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009.[16]	**Attempt is an offence (S. 84-C)** inclusion of this offence under the IT Act would be useful as while trying at the computer, like vandalising the data, hacking, in this condition, the accused can be punished for attempt to commit the crime in question.[17]

IX. Conclusion

Having said about the utilities of the technology on cannot gloss over the potential dangers associated with it. The increasing role of technology in the society and in business offers great lure to the criminals to exploit it. The truth is that they are successful in misusing this great medium for their nefarious activities, which led to a new genre of crime known as cybercrime. Through Internet computers are either being targeted for some crime or being used to carry out some crime. The internet is also being used increasingly for dissemination of objectionable materials like hate material and pornography.

---

[12] Inserted by S. 45 of the IT (Amendment) Act, 2008.Abetment is defined under S. 107 of IPC, 1860 as an offence.

[13] Section 69 of IT Act, 2008 provides direction for interception or monitoring or decryption

[14] Section 69-A of IT Act, 2008provides blocking for public access

[15] Section 69-B of IT Act, 2008 provides monitoring and collecting traffic data.

[16] Vide G.S.R. 782 (E), 27-10-2009.

[17] Inserted by S. 45 of the IT (Amendment) Act, 2008.Attempt is defined under S. 511 of IPC as an punishable offence.