Chapter 6

Necessity of a new legislation to deal with the Cyber-crime
Chapter 6
NECESSITY OF A NEW LEGISLATION TO DEAL WITH THE CYBER-CRIME

6.1 Introduction

In last preceding chapter, the Indian legislative framework to deal with Cyber crime in India has been analyzed. As Cyber-crime is now becoming reality in India, it needs comprehensive treatment to be dealt with. The pace of automation of government offices, computerization of banks, and adaptation of computer technology in each sphere of life, increasing number of Cyber cafes to have easy access to Cyberspace gives rise maximum risks where important data, information, digital money, intellectual property can fall in the hands of Cyber criminal.

Cyberspace is just as an open market place having digital money, property and valuable information easily reachable with thousands of gates, windows to enter without any gatekeepers and security guards. The Cyber crime has changed the age-old jurisdictional equation in Cyberspace. The world is now reduced into 'global-village' and artificial geographical national boundaries are now disappearing from the world map. However, the criminal laws are still jurisdictional based where local territory in which crime has committed is important criterion for fixation of criminal liability.

Unlike conventional communities, in Cyberspace, there are no policemen patrolling, gatekeepers restricting the entries or security guards controlling the movements, for the Information super-highway, leaving room open for virus transplantation, Cyber stalking, trademark counterfeiting and Cyber terrorism.

While the worldwide scenario on Cyber crime looks bleak, the situation in India isn't much better. There are no concrete statistics but reports say that Indian corporate and Government sites have been attacked or defaced
more than 780 times between February 2000 and December 2002. This is an 'Electronic Age' having electronic speed in transactions, trade and information sharing.

The printing culture and swiftly replacing by machine and the world is transforming from paper based to paperless society. The concept of Information technology is dawning in reality that is able to make this transformation possible. We are now creating new standards of speed, efficiency, and accuracy in communication, which has become key factor for boosting innovations, creativity and increasing overall productivity. Computers are extensively used to store confidential data of political, social economic or personal nature bringing immense benefit to the society.

6.2 Assessment of the Information Technology Act, 2000

6.2.1 Shortcomings observed in the Information Technology Act, 2000

No doubt, that India is pioneer country to legislate in the area of Computer and Information Technology, however, in the 6th year of its enforcement, the Information Technology Act, 2000 has revealed the mix reaction from different corner. No doubt, that it is masterpiece in itself, but charges can be conveniently labelled against it that the Act has certain inherent limitations and shortcomings and it fails on expectations. To discuss a few -

a. The Act does not refer to the protection of intellectual property like the Copyrights, Patents, or the Trademarks in the Cyberspace.

b. It is also silent on Domain-name infringement and Cyber squatting. This creates serious limitations directly reflected in the form of resistance on the part of corporate entities to invest in this area.

e. It extends the application of its penal provisions to persons outside India, irrespective of their nationality provided that the contravention takes place to the computer located within the territorial limits of India. Such extra-territorial jurisdiction is fraught with limitations as to its enforcement. Although, this seeks to afford protection for Indian Cyber space from intruders from other countries but the example of Dawood and Quattrochi clearly bare the ineffective enforcement machinery in India.

d. It excludes property transactions to be carried out on-line due to the necessity of payment of stamp duty and registration of documents.

e. The Act fails to address the issue of cross-border taxation that may arise in international contracts.

f. The question of jurisdiction of a particular country over on-line transactions, which involves more than one jurisdiction, has also been left open.

g. It does not deal with Internet privacy issues like prohibition of unsolicited commercial mail (spamming) and unauthorized use of private data collected on-line.

h. It binds digital signatures to the asymmetric encryption system, limiting the scope of innovation in technology. This is a serious drawback especially since the technology is being replaced with a more secure system soon.

i. It fails to cover control of Cyber laundering of money, which can easily be used for criminal or terrorist activities especially given the situation post September 11.

j. In recent phone taping scam of Mr. Amar Singh, leader of Samajwadi Party and others, it revealed the serious flaws with

---

respect to the provisions of Service Providers and intermediary. Now the law should have to give fresh look for fixing the non-optional responsibility and guidelines for ISP and intermediary. Both should not be allowed to flee away their legal responsibility by taking advantages of flaws in laws.³

Thus, on certain grounds the Information Technology Act, 2000 can be a better response to deal with the problems in Cyberspace. From Indian point of view, and keeping the statistics of Cyber crime under surveillance, it can be said that the level of Cyber crime in India is still within the controlling limit. Even today, it is matter of headline of the newspaper in bold letters if any incidence of Cyber crime reported. It is still not too common. Nevertheless, looking to the pace of growing speed of technology, in near future it will require thinking twice about the compatibility of the IT Act, 2000 with changing pace of the world.

6.3 Proposed Amendments in the Information Technology Act, 2000

6.3.1 A brief analysis and background

As discussed above, the present Act relating to Cyberspace prove insufficient on various grounds. During last five years from its inception, several new issues, legal disputes, and incidences took place, which require an urgent attention for its revival.

Amid the outcry over leakage of sensitive data from Indian BPO companies necessitating stringent privacy laws ushering in suitable data protection legislation among other things. The need for a data protection law has emerged again with a leakage of credit card information last week with an employee of a Gurgaon-based web-marketing firm at the centre of the scam.

The IT Act Review Expert Panel was set up for an in-depth review of issues relating to the Information Technology Act, 2000 in January 2005 year to consider suitable legislation for data protection, among other things. In fact the call for amendment was prompted by the controversy involving the arrest

³ Based on the Internet surfing and extracted from the material available on Internet.
of Baazee.com CEO in December 2004 in a case of sale of a sexually explicit clip on the auction site.

The industry had subsequently called for an amendment in the IT Act. Making the Baazee.com case as a reference point, the committee has been relooking at ways of balancing the rights of enforcement authorities with the rights of those who could be potentially accused.

The expert committee was headed by Brijesh Kumar, Secretary DIT, includes A K Chakravarty, Scientist-G, DIT, Kiran Karnik, President of Nasscom, Ajay Chowdhry, Chairman, HCL Infosystems Ltd, Ajit Balakrishnan, CEO, Rediff and R Ramraj, CEO, Sify Ltd.

The mandate of the committee included re-examining the IT Act so as to ensure that it remains an enabler for development of information and communication technology and has adequate measures for promoting growth of e-commerce and e-governance in the country and also for regulating Cyber crimes and Cyber forensics.

It has considered the recommendations made by the inter-ministerial working group on Cyber law & Cyber forensics and finalized the amendments to the Act; verified and analyzed suitable legislation for data protection (privacy) in the Act; reflected on the feasibility of making the Act technology-neutral.

It has also considered the issue of regulating Cyber cafes operations and blocking of web sites; and has looked into the matter of India signing the European Cyber Crimes treaty and make suitable recommendations.4

6.3.2 Brief summary of proposed amendment in the IT Act, 2000

The proposed committee submitted its report in August 2005 suggesting its proposed recommendations for an amendment in the Information Technology Act, 2000. The brief summary of the said committee-

Accessed on 22.02.2006 at 08.45.02.
Report of the Expert Committee Proposed Amendments to

The Information Technology Act, 2000

SUMMARY

August 2005

Department of Information Technology

Ministry of Communications & Information Technology

Government of India

New Delhi

1. The Amendments to the Information Technology Act, 2000 have been shown in revision mode with footnotes explaining the amendments.

2. As the technologies and applications in IT sector change very rapidly, some of the provisions related to parameters that may change from time to time have been amended to provide for the new developments to be incorporated by changes in rules/govt. notifications. This would enable the law to be amended and approved much faster and would keep our laws in line with the changing technological environment.

3. Sub-section 4 of Section 1 relates to "Exclusion". In view of changing needs, operation of this section has been made more flexible through prescription of such exception by rules rather than being part of the main Act.

4. The Act is being made technology neutral with minimum change in the existing IT Act 2000. This has been made by amendment of Section 4 of the Act to provide for electronic signature with digital signature as one of the types of electronic signature and by enabling the details of other forms of electronic signature to be provided in the Rules to be issued by the Central Government from time to time. This is an enabling provision for the Central Government to exercise as and when
the technology other than digital signature matures. Then there will be no need to amend the Act and the issue of rules will be sufficient. Consequently, the term digital is changed to electronic in other sections.

5. In Section 4, the main aspect of electronic signature for legal recognition, namely, its reliability have been provided consistent with the UNCITRAL Model on Electronic Commerce.

6. Section 6(2)(b) has been amended to allow public-private partnership in e-governance delivery of services.

7. A new Section 10 has been added for "Formulation and Validity of Electronic Contracts".

8. Relationship between CCA, CA and Subscribers (Sections 17 to 42) have been revisited on the basis of the recent operational experiences and certain amendments proposed.

9. In view recent concerns about the operating provisions in IT Act related to "Data Protection and Privacy" in addition to contractual agreements between the parties, the existing Sections (viz. 43, 65, 66 and 72) have been revisited and some amendments/more stringent provisions have been provided for. Notably amongst these are:

   (i) Proposal at Sec. 43(2) related to handling of sensitive personal data or information with reasonable security practices and procedures thereto

   (ii) Gradation of severity of computer related offences under Section 66, committed dishonestly or fraudulently and punishment thereof

   (iii) Proposed additional Section 72 (2) for breach of confidentiality with intent to cause injury to a subscriber.

10. Language of Section 66 related to computer related offences has been revised to be in lines with Section 43 related to penalty for damage to computer resource. These have been graded with the degree of
severity of offence when done by any person, dishonestly or fraudulently without the permission of the owner. Sometimes because of lack of knowledge or for curiosity, new learners/Netizens unintentionally or without knowing that it is not correct to do so end up doing certain undesirable act on the Net. For a country like India where we are trying to enhance the positive use of Internet and working towards reducing the digital divide, it need to be ensured that new users do not get scared away because of publicity of computer related offences. Section 43 acts as a reassuring Section to a common Ncitizen. The IT Act, 2000 in order to ensure that it promotes the use of e-commerce, e-governance and other online uses has been cautious not to use the word Cyber crime in the text.

11. Section 67 related to Obscenity in electronic form has been revised to bring in line with Indian Penal Code, 1860 and other laws but fine has been increased because of ease of such operation in electronic form; link-up with Section 79 of the IT Act, 2000 with respect to liability of intermediary in certain cases has been provided.

12. A new section on Section 67 (2) has been added to address child pornography with higher punishment, a globally accepted offense.

13. A new phenomenon of video voyeurism has emerged in recent times where images of private area of an individual are captured without his knowledge and then transmitted widely without his consent thus violating privacy rights. This has been specifically addressed in a new proposed sub-section 72(3).

14. A new Section 68(A) has been proposed for providing modes and methods for encryption for secure use of the electronic medium, as recommended by earlier Inter Ministerial Working Group on Cyber Laws & Cyber Forensics (IMWG).

15. Section 69 related to power to issue directions for interception or monitoring or decryption of any information through any computer resource has been amended to take care of the concern of MHA and also on lines with the recommendations of IMWG.
16. A new section 78 A (Examiners of Electronic Evidence) has been added to notify the examiners of electronic evidence by the Central Government. This will help the Judiciary/Adjudicating officers in handling technical issues.

17. Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases. EU Directive on E-Commerce 2000/31/EC issued on June 8th 2000 has been used as guiding principles. Power to make rules with respect to the functioning of the “Intermediary” including “Cyber Cafes” has been provided for under Section 87.

18. In order to use IT as a tool for socio-economic development, as explained in para 10 above, particularly to promote e-commerce, e-governance, its uses in health, learning, creating more opportunities for employment, reducing digital divide amongst others, it is necessary to encourage society to go through the learning experience. In order to enable this to happen, it has been made clear that the normal provisions of CrPC will apply, except that only DSP’s and above will be authorized to investigate the offences.

19. The amendment to the 1st Schedule (Indian Penal Code) and 2nd Schedule (Indian Evidence Act) around the recommendations of earlier IMWG has been incorporated. However, the term digital signature would be replaced by electronic signature at suitable places.

6.4 Is there any dire need of comprehensive legislation?

Today, we are sharing common Internet networking for all the economical transactions and information sharing. The enormous tentacles of optic fibers spread over the globe, which has led to set a scenario of new forms of transnational crime especially relating to Internet. New sets of situations exist now, which is capable of giving a speed of light to these transactions and trade. The virtual world has simultaneously developed a platform for Cyber criminals to commit crimes. The crimes committed in Cyberspace have virtually no boundaries and may affect any country across the globe. This, in
turn, has developed a dire need and growing concern amongst all for necessary legislation in all countries for the prevention of computer related crime.

Internet and Computer based commerce and communications cut across territorial boundaries, thereby creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries. This new boundary, which is made up of the screens and passwords, has separated "Cyber World" from the 'real world'. Territorially based law-making and law-enforcing authorities find this new environment deeply threatening.5

6.5 Computer related or computer facilitated crime - considerations

Computer crimes often extend into matters that are not crimes against computers, but are crimes facilitated by the use of computers. For example, theft is a crime in every legal system, and the criminal law should cover theft whether it occurs online or offline. Similarly, fraud is a crime, and ordinary fraud statutes will often use terminology that applies equally well to online conduct as it did to offline conduct. Other crimes, such as infringement of intellectual property rights or dissemination of child pornography also are not properly computer crimes - they are crime that may be facilitated by use of a computer. Before adopting a series of separate offenses 'facilitated by computer,' governments should examine their traditional criminal laws will cover offenses committed online. And to the extend that do not, rather than establishing separate offenses for computer related crime, it might be better to amend the general crimes laws to make it clear that they cover online conduct.

Nations may also want to consider how common concepts of the criminal law such as 'aiding and abetting' or 'attempt' apply to Cyber crime. Thus, if a nation's law has the concept of an attempted offense, then that concept might apply to Cyber crime. For example, launching a virus with intent to disrupt service might be a crime under the concept of intent even if the virus didn't work as intended.

Similarly, if a nation's law has the concept of aiding and abetting, that might be applied to Cyber crime, such that one who intentionally produces a virus and provides it to another knowing or intending that it will be used to destroy data or interfere with a system may be guilty of data or network interference caused by the virus even if the virus was introduced into a network by someone else.  

6.6 Two possible approaches to deal with Cyber crime

Today, the use and dependence of global society on the computer networking at national and international level generated an opportunity for trans-national computer crime. The global nature of computer networking makes it able for sophisticated criminals to operate from a distance and cover up or confuse the origins of their attacks. To respond to attacks in a timely and effective manner, system operators need to monitor user’s behavior and detect intrusions in real time. To identify suspects and launch investigations once a crime is detected, large-scale screening, tracing, and analysis of electronic evidence may be required.

It is therefore, utmost necessary to make our technological, economic and human resources compatible with each other and develops networking firewalls to protect Cyber space. States, as well as commercial and other public and private entities, face difficult trade-offs in allocating resources to fight Cyber crime. Increased network security and investigative measures may come at the expense of network performance, privacy, and users’ desire for anonymity.

It does not mean that the Cyber space can only be protected by international norms only. It may possible that private international laws may provide security laws and regulations for controlling of Cyber crime in Cyber space. It is only desirable at this stage that though States may also find their domestic laws, national security objectives, and political or economic priorities at odds with the conditions required for effective international

---

6 For more details, please see 'Trust And Security In Cyberspace : The Legal And Policy Framework for Addressing Cybercrime' August 2002, by GIPI (Global Internet Policy Initiative), A Project of Internex and the Center for Democracy and Technology.
cooperation. Restrictions on cross-border flows of information imposed for policing purposes may impede electronic commerce and other transactions.

There are two basic approaches to security in Cyberspace: a protective one and a reactive one. Each is constrained in different ways. The protective approach aims to deter criminals through measures that deny access to make a potential target less vulnerable to an attack. This approach is focused on defense.

It involves designing more secure Internet protocols, introducing trusted routers and virtual private networks, and utilizing firewalls, encryption, automated intrusion-detection systems, and other security measures. The reactive approach seeks to deter the threat through effective investigation, prosecution, and punishment.

Both approaches involve monitoring and diagnosing abnormal and unauthorized activity. The protective approach favours automation as well as oversight and decision-making by computer security experts. The reactive one depends more heavily on the participation of law enforcement and requires end user-oriented (rather than anonymous) traffic analysis, which may be as intrusive as scanning of attached files, keywords searches, and content filtering for signs of potential breaches of criminal law. Real-time investigative capabilities may extend to creating embedded data collection infrastructures and modifying hardware and/or software to provide for confidential law enforcement access to business, governmental, and private computer networks.

If we analyze both the approaches, it appears that both can be complementary. Their relative weights depend on the preferences and capabilities of implementing parties. Although there are significant obstacles

---

7 Neither exhaustive nor mutually exclusive, the two approaches provide a useful framework for evaluating with respect to civil liberties the technical and legal measures against cyber crime. Discussed at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, December 6-7, 1999.
9 Forms of this are being implemented by the Russian and U.S. Governments.
to achieving high levels of Cyber security, the protective approach is likely to facilitate greater security with less intrusion. The reactive approach may be more effective in cases of inadequate defense and in safeguarding users who are unable to afford, or unwilling to implement, sufficient protective measures. However, the reactive approach is inherently more intrusive and more threatening to civil liberties.

In short, both these two approaches have its merits and demerits. From the human right standpoint, it demand the opportunity of accessibility for each human being, without prior censorship. A chance should be given to each human being for use and effective application of technologies without denying it at initial stage where nobody is aware whether it will be used or misused by a person. Therefore, though reactive approach is inherently more intrusive and more threatening to civil liberties, it sounds strong argument that as a chance, first its experimental use should be permitted.

6.6.1 Objectives and riders for new legislation

With growing concern of world society for establishment of a suitable framework for trade and commerce and to have a safer environment, there is dire need felt for the emergence of a well-defined framework of Cyber Laws, which should be able to provide solid base to promote maximum use of electronic environment and tackle the incidences of its misuse. Thus Cyber Laws have expected to play duel role. First, to promote safer mode of use of electronic medium and other to control the activities attempting to misuse it.

Thus objectives before the legislations which require to be framed for Cyber-world is,

10 These obstacles include budget constraints, technical complexity, unclear responsibilities, security weaknesses in products, lack of awareness, lack of good security tools, lack of competent information security personnel, privacy and ethics issues, and legal or regulatory issues. Yet computer security requires a comprehensive and integrated approach, which extends throughout the entire information life cycle and recognizes the interdependencies of information security with such factors as system management, organizational management, legal issues, and physical and personnel security. See Dorothy E. Denning, Information Warfare and Security (Reading, Mass.:ACM Press and Addison - Wesley Longman, 1999), PP. 396, 397-400.
i. Create and implement a minimum set of guiding rules of conduct that would facilitate efficient communications and reliable Commerce through the use of Electronic medium.

ii. Define, punish and prevent wrongful actions that attack the electronic medium or harm others.¹¹

However, the case is very chronic because the field of Cyber space either completely lack Cyber Laws or rather delayed enactment and execution make problem more complicated in providing well-defined and comprehensive framework of Cyber Laws across the nation, if not across the globe. Speaking with example, interconnected networking of computers were started to appear on the scene well back in 1960s, but the regulating law in this sphere passed in late 1990s that too, only in USA. The rest of the society was still ignorant about the Internet. During this period, the society was using and misusing the technology and developing a sense of deviance either ignorantly or knowingly but setting some sort of anti-social behavioral pattern. With the potential world felt in the use of computer technology the problem was further aggravated as the steep rise in usage of Internet in the years followed after late 1990s. The post-modern ears witnessed steep rise in the use of electronic technology and soon mobile, computers, electronic machines was started to appear and being used for transactions and communication but with dire absence of any appropriate legal framework. And at the middle of last decade, the situations of formidable nightmares exist for the society and a mere it fumbling with its legal worn out tools creating great dilemmas what to do next to deal with this sort of criminality, popularly termed as "Cybercrime".

Some of the jurist has formed a view that there is not much necessity to give serious thoughts for the Cyber Laws. The justification commonly render that Cyber Crimes are merely an advancement or extended version of some of the traditional crimes only with the difference of presence of electronic technology. And thus need for separate comprehensive legislation is neither

inevitable nor warranted and the crime committed in Cyberspace can be tackled in the same manner as we used to deal with the traditional crimes. Surely this is true that the Cyber Laws scenario is globally more complicated than traditional laws due to the range of activities which are to be governed by these laws are largely technologically driven, an area which is dynamically changing and is beyond anyone’s control. The pace of technological development caused fast transformation of society and didn't wait for any responses and capable of entirely changing the scene. The Computer technology for example, has changed the old notion of money, banking, job works and even concept of man and machine relation. However, optimistically, enactment of these laws poses opportunities for nations to carve model Cyber Societies for the future thereby taking a lead in becoming Global IT Powers.

Not only the enactment of law for any alien new area is critical but its effective implementation is challenging as well. For generating the compatible environment for enactment and execution of law for society, the following the prerequisite postulates to be fulfilled:

i. To create a compatible climate so that society can respond in Self-Observance manner towards the legal framework creating workable model.

ii. Continuous surveillance at the level of various strata i.e. national and international level so that the model adopted should responsive with universality and informatively.

iii. Steady monitoring of the model with trustworthy feedback and cognizance.

iv. The feedback cognizance followed by the flexible adjudication with flexibility of accepting, incorporating and repairing with suitable modification and proper time and in justified way.

v. The Implementing Agency should be responsive to accountability-responsibility. At the same time, it should be
properly monitored that implementing agency would be properly guarded by research and techno-scientific aids.

In addition to the above postulates, it should be ensured that for the Cyber Law to be effective, Law is Simple, fair and full of clarity. Clarity and not the confusion should prevail the failing of which may lead to chaotic and mess situation. That further causes the misuse of law and harasses an individuals resulting in its defiance. The implementing agency will then be compelled to take corrective and coercive actions to ensure execution. This whole process may result in spread of corruption and polluting of the overall sentiments in society making the job of law implementing agencies more difficult for System Administrators to have a check on Frauds, Vandalism or Abuses, which may make the life of many online users miserable.  

6.6.2 A dream for Secure Cyberspace: need for comprehensive law

Thus, with the complex nature of Cyber-criminality, it is boon for the Cyber-criminals. Cyber-crimes can be committed from any location of the world, against any individual, institute or nation even without remaining present in the jurisdiction. This is beneficial for Cyber-criminals from many a ways to avoid or dodged the law enforcement agencies to bring him behind bars. The inter-connectively throughout the world with the help of Internet technology make Cyber-world as danger zone from security point of view and no-body can remain fear-free from constant threat of being victimize.

For civilized society, this situation is neither desirable nor allowed to be persisted too long and urgent steps to combat the social ordering are warranted. Therefore, it is essential to have a thought for Cyber-criminality from global point of view. It is, evidently, not the issues only threatening a particular nation, but total global community is on the target point of Cyber-criminality. Unfortunately though we have stepped in the new millennium,

our legal infrastructure is still needed entire innovations to suits present crime scenario. As various new challenges in the form of entirely different nature of crimes is mushrooming creating the havoc in this area. As commented by Malimath Committee Report...

"The last century has seen amazing change in the pattern of crime and the intensity and impact of the same on society. Terrorism has become global in nature, and the consequences of the same in terms of loss of life are phenomenal. Organized crime and its ramifications are global. Economic offences are transnational in operations and Cyber crimes have no geographical limitations. Sexual offences, child abuse, drug trafficking, trafficking in women and child, pornography, hijacking of aircrafts are all crimes which have no limitations either in terms of space or geographical boundaries and the impact of same affects the entire society and the nation itself. Therefore the need to combat these emerging crimes, which are bound to increase in number and in frequency, will have to be addressed and tackled. The existing laws are inadequate and therefore legislation and new policies of sentencing are the desideratum. Man's depredation of nature resulting in ecological imbalance, the concern for preservation of forests, wild life, compassion for the other living beings which are part of the Constitutional obligations have all resulted in new legislations being enacted. The increasing importance towards the end of the last century of human rights requires that punishments and sentencing should be consistent with Human Rights Jurisprudence. Rights of disadvantaged sections, gender bias, and sexual harassment in work places are all great concerns and elimination of all forms of discriminations [is] getting statutory protection and recognition."\(^\text{13}\)
Thus with the technological, commercial development it is expected that the legal system should also be renovated keeping pace with changing scenario. But to some extent the present criminal system is still witnessed the colonial impact and based on the age-old principles developed and codified by first law commission. Criminal law is the area which probably the oldest and least amended branch of legal system where the modernization is overdue.

6.6.3 Justification for separate Cyber Law for Cyberspace

The discussion on the point may start with the legitimate question that why at all there is dire need of separate and comprehensive legislation in the field of Cyber Law. There are already so many legislations prevailing and when the implementing agency has already been overburden. Again Cyber-Crime is another version of traditional crime in new variation with added element of technology. For deviance in human behaviour, control is important and whether comprehensive or fragmented legislation it may be - is irrespective. The argument can further be stressed that in criminality, it is the human behaviour which require to be controlled, irrespective of the fraction of legislation, therefore pressing for separate Cyber Law and separate infrastructure merely a baseless and unwarranted claim.

However, each coin has two sides and justification demand to have a thought for consideration of other side. First and basic argument of those raising their voice for separate Cyber Law starts from completely ruled out the basic assumption that Cyber Crime is another version of traditional criminality with slight variations. Though superficially it appear that Cyber Crimes are on certain footing resembles with traditional criminality does not make it similar and less serious. Because when computer technology added to the act of commission of crime, it step out of jurisdictional limits and act become global from local. This makes a considerable difference. Again the problem of identity, concept of

---

headed by Dr. Justice V.S. Malimath, formerly, Chief Justice of Karnataka and Kerala High Courts. Point no. 14.6.1 PP. 174-175.
illegality is also makes impact which require to be considered Cyber Crimes totally and entirely on different footings.

Next argument is based on the consideration that when the global society is sharing common network of computers, there should be uniformity, universality and required minimum common standard for global community. Thus, in Cyberspace should be the area where the international legal standard are in operation and common minimum global rules are in operation sanction and agreed upon by each national law making authority. Thus, if we want to deal Cyber Crime not only at national level, but also want to tackle it in conformity with international norms, there should be a comprehensive legislation compatible with international agreed norms.

Further arguments may be stressed that criminal laws are not only related with the norms controlling human behaviour. Crime is relative phenomenon the indexes of which differ from nation to nation. It again attracts the policy, procedure, extradition laws, and international policing to make Cyberspace safer space. Thus declaration of Cyber Crimes, procedures and punishment should in such a way which may promote workable model. Otherwise, the confrontation amongst the national criminal procedure and lack of agreed standard and lack of extradition treaty will make it difficult to deal with.

The need for the comprehensive legislation in the Cyberspace may also assume significance looking to the fact that the phenomenal spread of Internet has been enabled mainly due to the absence of a centralized regulating agency. Anyone who has access to a computer and a telephone network is free to get hooked to the Internet. This uncontrollable growth of the Internet makes the need for regulation even more badly felt.\(^\text{14}\)

The claim for security in Cyberspace also strengthens on another account. Internet security strengthened the spirit of nationalism because

---

it is protection of information from divulusive action, which unauthorized
disclosure modifications, or loss of data, dis-information of denial of data
system services. Defense from country from within or without depends
on information security. There are mainly four areas of information
systems where security counts immeasurably -

1. Financial system
2. Security on the internet
3. Security in the personal and data communication
   systems, and
4. Software security\(^{15}\)

Presently the criminal procedures across the world are fragmented
into national models which differ according to countrywide socio-political
and economical rider.

This gives rise to many different rules governing the behaviour of
for Computer and Internet Users. Most of the websites allow the users to
join or leave free of cost.

The rules are comfortable and user has to just click "I Agree" on
the screen where certain rules and regulations are given. This terms and
condition which bind users in one sided way are most of the time glanced
away without any importance. Again these websites do not take pain
about the identity of user, his qualification or disqualification and
everything is going on mutual understanding.

Thus Internet traffic is most risky without any suitable legal
framework and there is no policing, no any mechanism to check and users
most of the time use fake identity. It is now possible to trace the phone
number wherefrom the access has been made, but in case of Cyber café
and other places of public use, the things again become more complicated

\(^{15}\) Rauttaro (Dr.) R.L., 'Gazing into the new millennium communication territory' Published in
compilation compendium entitled, 'Globalisation and Indian Economic - Issues, Strategies
to fix the criminal liability. Under the present situation it is difficult to check on Pornography, Cyber Stalking, Internet Frauds, Vandalism, virus transplantation and abuses which may make the life of many online users miserable.

This situation is alarming as any element of distrust for Internet may lead to people avoiding doing transactions with online sites thereby directly affecting e-Commerce growth. The Mis(Use) of Internet as an excellent medium of communication may in some situations lead to direct damage to physical societies. Non-imposition of taxes on online transactions may have its destructive effect on the physical business and also government revenues. Terrorists may also make use of web to create conspiracies and make violence in the society.\(^{16}\)

Therefore, as the world is swiftly switching over to electronic machine and we are one or the other way stepping into the Cyberspace it is essential that artificial life of control between real world and Cyber world should be pushed off and all or some of the feasible rules of real world must be made applicable to Cyber world also. The Cyberspace should be brought in the umbrella of external compulsion for monitoring online transactions and the Cyber world for preventing any instability.

6.7 Basic approaches for creation of Cyber Laws

Following are the basic approaches for creation of Cyber Laws, which will ensure the smooth governance of Internet globally:

a. Formulation of new laws and amendment of existing laws by nations within their present territorial boundaries thereby attempting to regulate all actions on the Internet that have any impact on their own population.

b. Nations may enter into multi-lateral international agreements to establish new and uniform rules specifically applicable to conduct on the Internet.

c. Creation of an entirely new international organization, which can establish new rules and new means of enforcing those rules.

d. Guidelines and rules may naturally emerge from individual decisions like domain name and IP address registrations and by websites and users deciding about whom will they patronize.

All these approaches have their own merits and demerits.¹⁷

In order to combat the challenges and threats and create counter mechanism to deal with the same, many nations have determinately coming forward with best software, hardware and other police mechanism. And no doubt that it is possible by computer technology including telecommunication to control the Cyber deviance.

The further attempt has also been made to modify and modernize the respective domestic criminal laws so as to prevent the Cyber and computer crimes.

However, these all attempts have been yet made within the respective boundaries of the nation except the collective attempt by European Council to prepare law for the European Zone. However, as the problem is globally concern, any best attempt to resolve it locally may not leads to effective controlling and there is need to create legal mechanism suitable at national level and compatible with international as well as foreign legislative norms.

Again it can be seen that yet no country has fully resolved all the issues such as legal, enforcement and prevention of crime. The

legislations enacted by different countries cover only few of the classified computer-related offences. However, looking to the dynamic and fast changing technology, new types of offences may pop-up frequently.

Let's now once again review the alternatives available for establishing a comprehensive legal framework. Can we make only territorial laws applicable to online activities that have no relevant or perhaps even determinable geographic location?

It seems to be very difficult. We must also allow responsible participants on the Internet to set their own rules and to help all concerned (online and offline). The law of the Internet has already emerged, and we believe, that it, will continue to emerge with individual users voting to join the particular systems they find most congenial.

However, this model also does not solve all problems, and various governance issues cannot be resolved overnight. We will need to redefine Cyber Legal processes in this new dynamic context.

Finally, the Cyber Law defined as a thoughtful group conversation about core values and distinct benefits to the Society will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically defined territories.  

6.8 Conclusion

Therefore, keeping changing pace of the world scenario, it is necessary to have a comprehensive Cyber legislation, which can govern Cyber world as well as legitimize transactions, strengthen law and order situation and provide effective execution. As the Cyber world is multi-jurisdictional space, the compatibility of the heterogeneous jurisdiction is utmost necessary.

Therefore, harmonizing the conflicting issues of various legal systems should also be taken into consideration and new foundation of

---

Cyber-Laws should be laid down keeping these entire objectives in mind. However, it is irrespective here that whether such comprehensive legislation touching the issues directly or indirectly.

Today, not only the globalization, but changes are occurring into the legal approach of each legal system both from within and from outside. The old age notions of controlling citizenries and non-optimal characteristics of legal norms without justification saying, 'Sovereign command backed by sanction', has already been given a back seat. Today new legal order is taking a shape where there is lot of scope for individual liberty, and international order also going to be influenced each national system. 'Vishakha' case is the best example of it. Under this backdrop, the new riders for comprehensive legislation should be thought for dealing the problems of Cyberspace.