Legal and Regulatory Challenges in Combating Financial Cyber Crimes

Rajat Bhatia[1]*, Dr. Aparna Soni[2]

[1] Research Scholar, University of Technology, Jaipur, Rajasthan, India

[2] Associate Professor, Department of Management, University of Technology, Jaipur, Rajasthan India

Abstract - In today's modern world, cyberspace is increasingly exerting its influence over every aspect of human endeavour. The internet is bringing about a major and irreversible shift not just in the economic environment but also in the underlying premises upon which enterprises are founded. E-commerce has emerged as a key component of the new electronic economy that has emerged as a result of this transformation of the industrial economy. Cyberspace is the domain that can be found behind the computer screen, on the other side of the telephone receiver, and just a centimetre beneath the surface of the keyboard. It is a place where all types of coded phenomena, including words, sounds, and images, may be found dancing. In principle, cyberspace has no limits whatsoever. Everything that can be reduced to zeros and ones will ultimately find a home here; this includes everything that can be measured, defined, and traded. With the increased dependence on e-commerce and e-governance, a wide variety of legal issues related to use of the internet as well as other forms of computer or digital processing devices have emerged. These issues include violations of intellectual property, piracy, freedom of expression, jurisdiction, and others, and they need to be tackled through the interdisciplinary field of information law. In the present new millennium, information technology advanced by computer network undoubtedly pervades every aspect of society and governance.

Keywords - legal, regulatory, challenges Financial, Cyber, Crimes

- X -

INTRODUCTION

The advancement of information and communication technology, sometimes known as ICT, has been a primary factor in the development of modern civilizations. They are the bedrock upon which the social, economic, and political development of individuals, organisations, and governments is built. Not only can you find them everywhere, but development simply cannot be made without them. The next generation of networked societies is being advanced by a wide variety of technologies, including, but not limited to, smart gadgets, M2M communications, and cloud-based services. Because they provide major benefits such as increased productivity and speed, decreased costs, and more flexibility, digital technology and internet connectivity are currently undergoing a process of systematic integration into all verticals of both the commercial and governmental sectors.

Cyber Crime Legal Regulation

Salmond, a prominent English jurist, made the astute observation that the purpose of the law is to control the behaviour of individuals within the context of the community.

Need for a Cyber Law

With the increased dependence on e-commerce and e-governance, a wide variety of legal issues related to use of the internet as well as other forms of computer or digital processing devices have emerged. These issues include violations of intellectual property, piracy, freedom of expression, jurisdiction, and others, and they need to be tackled through the interdisciplinary field of information law. In the present new millennium, information technology advanced by computer network undoubtedly pervades every aspect of society and governance. 105 Since cyber space has no geographical constraints or bounds nor does it have any physical qualities such as sex, age, etc. it offers a huge difficulty before the law enforcement authorities for regulating cyberspace transactions of citizen with in a country's territorial jurisdiction.

Despite the fact that, in all actuality, a user of the internet is subject to the laws of the state from which the individual accesses the internet, this overarching principle can become complicated when the issues at hand are of an international character. It is a fact that while computer technology was still in its infancy and still in the process of evolving, no one ever gave any thought to the possibility that users of the internet may inadvertently exploit it for illegal reasons. Because of the anonymity of its character and least possibility of being detected, the cyber criminals are misusing the computer for a variety of crimes which calls for the need for an effective legal framework and regulatory measures to prevent the incidence of this peculiar type of criminality which is rampant in cyber space.

Cyber Laws of Various Countries

In response to the issues posed by illegal activity conducted online, the legal systems of many nations have included cyber law into their framework. While the cyber laws of certain countries have been extensively updated, those of other nations have only been partially updated. However, there are a handful of nations that have not yet begun the process of adopting cyber laws to tackle crimes committed via computers and the internet.

Because cybercrimes do not respect physical or territorial limits, it is possible for them to cross national borders, which poses a significant risk to nations whose legislative safeguards against this type of crime are inadequate. Because various countries' local cyber laws overlap and differ, it is difficult to determine whether or not international cyber offenders will be prosecuted. In a nutshell, the international community has categorised all cybercrimes as falling into one of 10 categories that are considered to be of a global character. It is possible to classify them into the following four primary categories:

1. Data-related cybercrimes, which include interception, modification and theft of data ;

2. Network related cybercrimes including interference and sabotage of network e.g. distributed denial of service attack (DDoS) ;

3. Crimes related to access such as hacking, virus distribution etc.; and

4. Computer related crimes including computer fraud, computer forgery and aiding or abetting cyber criminals.

Technology and Information Exchange on a Global Scale

In this day and age of globalisation, there is a dramatic change in human life that has led to tensions in every sphere of life, the tensions, such as between the need to both decentralise and centralise, the desirability of being simultaneously a leader and a follower, an individual and a team player, etc. In this day and age of globalisation, there is a dramatic change in human life that has led to tensions in every sphere of life, the tensions, such as One such paradox, which encompasses the shift that is taking place now and is at the centre of it, is the global paradox. According to this paradox, the larger the global economy, the more powerful its tiniest actors become. The social values are experiencing a quantum change as a result of globalisation and the transition to the third wave, which is resulting in the thinking process that man, although becoming universal, wishes to stay provincial in the areas of culture and government.

Despite the fact that the desire of man to strike a balance between the particular and the general has always existed, the revolution in communication technologies has pushed this issue to the forefront. The human viewpoint has shifted as a result of the development of the information era that we are living in, shifting from "Think Globally, Act Locally" to "Think Locally, Act Globally." The emergence of a new age of provincialism has contributed to the development of hostilities in many different regions of the world; nevertheless, this fresh viewpoint comes with its own set of challenges as well. On the political stage, left vs right has given way to local versus global or universal versus provincial as the primary dividing line. As a result of the worldwide change away from the role of the state toward the value of the individual excellence, which is riding on the wave of the revolution in telecommunication, the chances for individual freedom and entrepreneurship are completely unmatched. In point of fact, this has opened up new avenues of opportunity and entrepreneurialism for individuals, which in turn gives rise to new ideas of individuality and provincialism, which leads to disputes.

The Growth and Evolution in Information Technology

Changing technology is driving the next wave of economic growth. To take advantage of that growth, we will have to not only apply new technology but also new thinking. Data are the basic building blocks of the information economy and knowledge-based business. In the early years of this economy, we focused on data that came to us in four particular forms: numbers, words, sounds and images. What we did with that data-how we processed, stored or otherwise manipulated them, determined their value. Information is data that have been arranged into meaningful patterns and knowledge, which helps in application and productive use of information. Tomorrow we shall see knowledge superseding information as the information had superseded data earlier. The shift from information to knowledge, however, is giving rise to a different phenomenon; awareness of the value of knowledge is exceeding the ability of many businesses to extract it from the goods and services in which it is embedded. Those who can figure out and utilize will derive as much power and profit from the knowledge as data and information brought in their turn. The development of knowledge-based business is a reflection of an even larger transformation occurring in our society. The last decade of 20th century had witnessed Information Technology (IT) emerge as the most prominent technology, which have a revolutionary effect on the lives of the people across the world.

Cybercrime and the Law

The surge in reported occurrences of cybercrime in India has presented the country's law enforcement officials with a new set of difficult issues. Through the development of information technology, actual individuals have been able to completely transcend physical barriers. The old adage that every coin has two faces is absolutely correct. The new digital global community, which sprang into existence at the speed of light, comes with a plethora of benefits as well as a number of potential drawbacks. Over the course of more than a century and a half, India's criminal justice system has matured into what is widely regarded as one of the most effective judicial systems in the world. This reputation has gained India widespread respect on the worldwide stage. Parliament, which is responsible for making laws, the police, which are in charge of enforcing those laws, prosecutors, attorneys, and judges make up the essential entities involved in the administration of criminal justice. They have a significant amount of functional independence, but because their operation is based on the principle of checks and balances, it prevents them from intruding on the territory of the other party and ensures that they work in total coordination with one another.

Judicial Trend in India

It is necessary to emphasise that Indian case law on cyber jurisdiction of the courts was almost non-existent prior to the enactment and enforcement of the Information Technology Act, 2000 on October 17, 2000. This is something that must be stated. The growth of information technology in the new century as a faster and quicker method of communication has led to various unintended effects that have resulted in cybercrimes being brought before the Courts for adjudication.

In the case of P.R. Transport Agency v. Union of India and others,5, the question of whether or not a court has the authority to hear a matter in which a contract has been established between parties residing in separate locations through the use of e-mail was at issue. In this particular instance, Bharat Cooking Coal Ltd. (BCCL) conducted an online auction for various quantities of coal, and the offer that the plaintiff (P.R. Transport agency) submitted for 40,000 metric tonnes of coal sourced from the Dobari colliery was accepted. On July 19, 2005, the BCCL informed bidders via email that their proposals had been accepted. In response, the plaintiff deposited the sum of 81.12 lakhs by writing a check payable to BCCL. BCCL received the cheque and paid it, but they did not provide the plaintiff with the coal that was promised. Instead, it (BCCL) informed the plaintiff of the cancellation of the aforementioned e-auction by e-mail contact, citing "certain technical and unavoidable reasons."

The plaintiff discovered that BCCL had cancelled the online auction for the sale of coal because there was another person whose bid for the same was higher than the one that had been considered earlier due to some flaw in the computer or its programme or the feeding of data. This person's bid had not been considered earlier because of the flaw. In the case that was brought before the High Court of Allahabad, the plaintiff, P.R. Transport, contested the legitimacy of the defendant's decision to cancel its contract. The defendant, BCCL, raised an objection to the territorial jurisdiction of the court on the grounds that the High Court of Allahabad did not have jurisdiction in the case because the cause of action had not arisen in the state of Uttar Pradesh. The defendant's argument was that the court lacked the authority to hear the case.

OBJECTIVES OF THE STUDY

1. To study on Technology and Information Exchange on a Global Scale
2. To study on Cyber Crime Legal Regulation

RESEARCH METHOD

Data analysis is primarily used to analyse information in a fair and impartial manner, to provide analytical conclusions that are convincing, and to rule out alternative potential interpretations. When choosing the most suitable statistical techniques, several factors must be taken into consideration.

Research Design

Data collection is done so that decisions may be made about key issues, records of information can be kept, and information can be communicated to others. Information on "Financial Cyber Crime and its Management" was the primary focus of the data gathering process early on.

Data Collection

The process of collecting data is generally started early on in a project to improve anything, and it is frequently formalised by making a plan for collecting data, which frequently includes the activities described below. Pre-collection activity, which occurs before any data gathering, is one of the process's most crucial steps. It is sometimes not noticed until it is too late that the value of the information collected from their interviews is greatly diminished due to a poor sample of both questions and informants as well as insufficient elicitation procedures. After all pre-collection tasks have been completed, field data collection, whether it involves interviewing participants or using another method, may be done in a way that is systematic, methodical, and scientific. Having a record of the information, being able to make decisions about important issues, and sharing knowledge with others are the objectives of information collection. The initial aim of the data gathering was to provide details on "Financial Cyber Crime and its Management."

DATA ANALYSIS

The criminal justice system faces a number of obstacles.

In most cases, the changes brought about by advances in technology are reflected in new laws. The fast development of technologies such as the internet, on the other hand, poses an obvious risk of rendering the legislation obsolete. Internet is a global network of computers that is built on TCP/IP and other high-speed communications protocols. There are thousands of nodes on the internet, and millions of people utilise it. The rest of the world views the internet as an innovative and interesting new means of communication. The primary functions of the Internet are to communicate via e-mail, to facilitate the transmission of data between computers, and to provide remote access to local systems. Since the 1980s, digitization and the widespread availability of low-cost personal computers have made copying simple, perfect, and quick. This is true regardless of the number of generations of copies that have been made, the method by which the information is stored, or the number of people who are copying it. Because it is now feasible for anybody with a personal computer to make thousands of flawless copies in a short amount of time, the only thing standing in the way of widespread copying is access to content that is worth copying.

The advent of advanced communications networks such as the internet has made it possible to virtually access content that is worthy of being copied. Unfortunately, because to the vast amount of information that can be sent, the open and uncontrolled nature of the internet, and the fact that the location of the user is irrelevant, the internet also serves as a fertile field for criminal business. Because the internet is made up of computers, any illegal activities that take place on the internet are referred to as "computer crimes." The concept of a "digital crime," however, is difficult to pin down. It is possible for a computer to be either the target of a criminal act, such as when it is stolen or damaged, the scene of a criminal act, such as when it is used to commit fraud or an infringement of copyright rights, or the instrument of a criminal act, such as when it is used to illegally access other machines or store information.

Crimes Committed Online

The question that needs to be asked now is, "What exactly is cybercrime?" The definition of cybercrime is fraught with a lot of difficulties. The first challenge is to offer a definition of cybercrime, as at this moment in time there is no definition of cybercrime that is globally acknowledged or that is accepted uniformly. This is not surprising when one considers the various national legal traditions that exist in the various countries of the world, as well as the fact that the term "cybercrime" is used as an umbrella term to refer, at least in part, to a very recent set of activities that have not yet been fully incorporated into the legal systems of the various nations of the world. The terms "computer crimes," "computer misuse," and "IT crimes" are almost always used in conjunction with the term "cybercrimes." Because of this, the term computer-related crime is increasingly being used in place of the more traditional phrase computer crimes. The second issue is that there are not enough reliable and comprehensive data. There is a lack of accessible reliable quantitative data that can offer a comprehensive picture of cybercrime. The United Nations Manual states that law enforcement officials believe that the reported computer crime figures do not accurately reflect the real number of crimes committed using information and communication technology (ICT). There aren't enough statistics available on cybercrime for a few of different reasons. The first reason is technological, and it is based on the vast storage capacity and the speed of computers. Because of these factors, which make it very difficult to identify computer crime, some victims are unaware that they have been a victim of a cybercrime until they are notified of this fact.

Penalty for Failure to Furnish Information Return etc.

If any person who is required under this Act or any rules or regulations made there under to-

(a) If the person is required to produce any document, return, or report to the Controller of the Certifying authority and he or she fails to do so, the person will be subject to a penalty that cannot exceed one lakh and fifty thousand rupees for each instance of such failure;

(b) File any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file any return or fails to furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which he is in violation of this provision. similar failures continue;

(c) Maintain books of accounts or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

This section makes the person who is required to file any return or furnish any information, books or other documents to the concerned authority or maintain books of accounts or records, but fails to do so, liable for contraventions and provides monetary punishments for the same. The person is required to file any return or furnish any information, books or other documents to the concerned authority.

Residuary Penalty

Whoever violates any rules or regulations made under this Act, for the violation of which no separate penalty has been provided, shall be liable to pay a compensation amounting to not more than twenty-five thousand rupees to the person affected by such a violation. This compensation amount may not exceed the amount that would have been paid had the violation not occurred.

Protected System

1. Any computer, computer system, or computer network may be designated as a protected system by the applicable government by the publication of an official notification in the Official Gazette.
2. The competent government may, by order in writing, permit the people who are authorised to access protected systems that have been notified under sub-section (a) (1).
3. Any person who obtains access to a protected system or makes an attempt to obtain access to such a system in violation of the provisions of this section shall be punished with imprisonment for either description for a term that may extend to ten years and shall also be liable to a fine. The maximum term of imprisonment for either description is ten years.

The following are the essentials to make a person criminally liable under this section:

1. The appropriate Government should have declared any computer, computer system or computer network to be a protected system.
2. Such declaration should have been made by the appropriate Government through notification in the Official Gazette. The intruder secured access or attempted to secure access to the notified protected system in contravention of the provisions of this section
3. The intruder should not have been authorized to access the notified protected system.

A declaration by the Government notifying a computer, computer system or computer network to be protected system can be made in the interest of the Sovereignty of India or the state concerned, defence, public security, state integrity and financial, economic and commercial security or friendly relations with other nations.

Attempt to secure any illegal access to the protected system has also been made punishable under section 70 (3). Therefore, it is immaterial to determine whether the attempt was successful or not.

CONCLUSION

The internet provides instant communication between any computers that are linked to it, point-to-point communication, and offers an expanding number of private and public communication options. The Internet is a worldwide resource that connects millions of users using a standardised set of protocols. These protocols are a form of communication that is mutually agreed upon between the parties involved. In today's modern world, cyberspace is increasingly exerting its influence over every aspect of human endeavour. The internet is bringing about a major and irreversible shift not just in the economic environment but also in the underlying premises upon which enterprises are founded. E-commerce has emerged as a key component of the new electronic economy that has emerged as a result of this transformation of the industrial economy. Cyberspace is the domain that can be found behind the computer screen, on the other side of the telephone receiver, and just a centimetre beneath the surface of the keyboard. It is a place where all types of coded phenomena, including words, sounds, and images, may be found dancing. In principle, cyberspace has no limits whatsoever. Everything that can be reduced to zeros and ones will ultimately find a home here; this includes everything that can be measured, defined, and traded. The boundaries of cyberspace are inconceivable to define using traditional geographical categories. It is a fact that can be situated 'nowhere,' despite the fact that its presence may be sensed 'everywhere.' The proliferation of global electronic communications has produced new domains, each of which will eventually have its own unique set of rules.

REFERENCES

1. Kamal Ahmad : The Law of Cyber-Space (U. N. Institute of Training & Research) 2006.
2. Dr. Amita Verma : Cyber Crimes and Law (Central Law Publications) 2009.
3. S. K. Bansal : Cyber Crimes (A. P. H. Publishing Corporation, Delhi) 2003.
4. Dr. R. K. Chaubey : An Introduction to Cyber Crime & Cyber Law (Kamal Law House Kolkata) 2008.
5. Dr. Farooq Ahmad : Cyber Law in India : Law on Internet, 2nd Edition (Pioneer Book Publication, Delhi) 2005.
6. Nandan Kamath : Law Relating to Computers Internet & Commerce, 2nd Edition (Universal Law Publications Co. Delhi) 2000.
7. Rahul Mathan : Law Relating to Computers and Internet (Butterworth, New Delhi) 2000.
8. R. C. Mishra : Cyber-Crime : Impacts in the New Millennium : Ist Ed. (Author's Press, Delhi) 2002.
9. R. Nagpal : What is Cyber Crime ; (2003)
10. B. B. Nanda and R. K. Tiwari : Farensic Science in India : A vision for 21st Century (Select Publishers Delhi) 2001.

11. Ashish Pandey : Cyber-Crime - Deviation and Prevention (J.B.A. Publications) 2008.

12. Dr. N. V. Paranjape : Criminology & Penology : 14th Ed. (Central Law Agency, Allahabad) 2008.

Corresponding Author

Rajat Bhatia*

Research Scholar, University of Technology, Jaipur, Rajasthan, India