ABSTRACT

Crime is not a static concept and hence the criminal law has to be modified or amended as per the demanding and changing circumstances and needs. Today, in the advanced environment of science and technology and the advent of information technology at gross root level, criminals became more sophisticated and the crimes have turned to more complexity as their modus operandi is no way synchronized to the traditional methods of crime investigation. The Indian judicial and legal systems also need to take on as per the current information technology oriented society. The present research study aims to examine the procedural aspects of investigation under the context of cyber crimes in India and it studies the investigation machineries under the ambit of cyber crimes. This study further assess the methods and process of investigation under the IT Act, 2000 and amendment act, 2008 and it analyzes the challenges and practical problems faced by the investigation authorities in the process of cyber crime investigation. The present research design comprises the doctrinal approach in its application. An academic effort has been made to undertake the proportional analysis of various investigative mechanisms and procedures those involved in the detection of cyber crimes under the IT Act, 2000. This research study had concluded that though there exists new provisions covering the investigative procedures under cyber laws, many new milestones in terms of technology and digital process have to be reached by the investigating agencies and this requires appropriate training and logistic support for the cyber law implementing authorities and cyber law regulatory bodies.

KEY WORDS: Cyber Crime, Investigation, Challenges, IT Act, 2000

1. INTRODUCTION

In the matters of crime, there exists several stages of criminal proceedings. Among them, the courts are concerned with the stages of inquiry and followed by trial procedures. It is said that the term inquiry is having a much wider scope. Trial procedures begins in those acts which are said to be crimes. Any how, the inquiry and trial can take place whenever the process of investigation is said to be completed. Thus, the criminal proceedings comprises the stages of investigation and inquiry followed by trial procedure. The stage of investigation starts whenever the information of crime reaches the police department and it is said to be the origin point of criminal law. There may not exist the unified and unique process of investigation all over. The investigation authorities will apply multifarious detection techniques while carrying out the investigation procedures of any crime. It is aptly said that investigation process is skill oriented and hence it needs the special and specific knowledge with regard to the existing subject matter in question. Broadly we can say that the same set of procedures required and applicable to both conventional and cyber crimes and the later involves the application of skillful techniques. The code of criminal procedure encompass the procedural aspects of crime investigation. Generally, regular methods will be used for investigating the conventional crime. The agencies of law enforcement were bound by certain basic procedural aspects and set of Rules and Regulations. They are said to be the procedures of established nature for investigation and prosecution of various types of crime. In traditional crimes, physical evidences are available in general to the investigation authorities at the crime place and their collection of physical evidence requires little technical knowledge and a lot of common sense. But it is not the same in the case of cyber crime detection as it involves special skills and
tools of scientific nature without which investigation procedure will not be possible. Keeping these things in view, the Indian legal system had introduced certain specific provisions of investigation under the context of cyber crime. The Information Technology Act, 2000 was bound to amend certain existing provisions of Criminal Procedure Code(CrPC) and Indian Evidence Act. It has amended certain provisions of investigative mechanisms under the aspect of cyber crime investigation. According to the CrPC, section 2 (h), investigation comprises all the proceedings under the code for collection of evidence by the police officers or by any person other than magistrate who is authorized the magistrate. Section -157 of CrPC provides the investigation procedure which says that the station house officer has to proceed to the crime spot to investigate the facts and circumstances of the case and if necessary takes measures for the discovery and arrest of the offender. It mainly comprises the facts ascertaining nature and assorted circumstances in relation to that case. Generally the investigation ends with the police report submitted to the magistrate as prescribed under CrPC , Section 123 of the code.

II. STATEMENT OF THE PROBLEM

The main purpose of any criminal investigation is said to be the finding of the truth or allegations made otherwise in the information given in the form of first information report (FIR) and subsequently the judicial courts have no authority to make inquiries into the allegation made therein in the form of first information report and for quashing. A charge sheet will be submitted by the investigating authority upon completion of the investigation process and the competent judicial court may take the cognizance of the offence if the same was disclosed by the evidential material collected in the process of investigation and it is said to be that it is only when cognizance is taken by the court that court will acquire the jurisdiction power to decide the matter on the merits of the respective case parts. At the same time the court can order the quash orders on the investigation procedures on the ground that any case of mala fides made out against the investigation agency.

In the present day circumstances, the criminals are resorting to the use of digital techniques and skills in order to commit the crimes and this made the present day investigation procedures very problematic to the investigating authorities and it had paved the way for hectic workload schedules for the police department in India. Therefore there is every need on part of the said police investigation agencies in order to develop the skills and techniques to counter act and trace the evidentiary aspects in the criminal cases and a skillful and tactical logistic development is to be done from the investigation procedural aspects.

With the advent of information technology and other digital communication techniques and logistical support, all the governmental agencies are moving ahead towards the digital world and information technology platform. But, in comparison with other existing governmental departments, the police investigation authorities and agencies are not equipped with the innovative and modern technologies and other support skills to get synchronized with the present day cyber crime prevention and still the said police department are struggling with age –old office working systems and investigative mechanisms.

The prevailing Indian investigation authorities and agencies are still practicing the obsolete tools of investigative procedures. Even it may be stated as the reason for the low conviction rate in India. The aspect of police and criminal investigation system are said to be the subjective matters of the state government and it is the sole responsibility of the state mechanism to update their skills and technologies of their respective police departments and they are authorized to equip the required logistic support to the concerned investigation personnel.

In the recent times, steps are being taken by the corresponding investigation authorities in order to equip themselves with the required formats of information technology skills and digital applications. This will certainly reduce the investigation time periods and other unnecessary paperwork procedures. The implementation of information technology act, 2000 had clearly made certain provisions for the innovative investigation mechanisms under the context of investigation procedure as laid down under the traditional provisions of criminal procedure code. In this context, it was felt necessary by the researcher in order to compare the investigation procedures under the conventional law and cyber law under the provisions of information technology act,2000.

OBJECTIVES

1. To examine the procedural aspects of investigation under the context of cyber crimes in India
2. To study the investigation machineries under the ambit of cyber crimes.
3. To assess the methods and process of investigation under the IT Act, 2000
4. To analyze the challenges and practical problems faced by the investigation authorities in the process of cyber crime investigation.

III. RESEARCH METHODOLOGY

The present research design comprises the doctrinal approach in its application. An academic effort has been made to undertake the proportional analysis of various investigative mechanisms and procedures those involved in the detection of cyber crimes under the IT Act, 2000. Comparative analysis pertaining to the investigation procedures under conventional crime and cyber crimes will be carried out by verifying various provisions under the code of criminal procedure and Information Technology Act, 2000.

IV. INVESTIGATION MECHANISM UNDER THE AMBIT OF CYBER CRIME

In the Indian judicial system, the process of executing the law is solely dependent on the executive wing. The police departments generally discharges the execution duties of various provisions of legal rules and regulations made from time to time. In other words, the executive branch is the sole discharging agency of the law of the land. The executive works under the directions of the judicial system in its process of discharging the duties and obligations.

In India, the judicial system provides the requisite mechanism for investigation. The emergence of cyber crime in India is a major threat to the legal and judicial systems and it has developed the ability to tackle the cyber crimes effectively and efficiently. As the modern society is said to be the information technology oriented society, the Indian judicial system has to adopt the required and the needed investigative mechanism in terms of cyber law and cyber crimes. It is a well known fact that majority of the cyber crimes in the country were not reported due to the ignorance of the public towards the cyber crime provisions and set of other legal regulations.

The information technology act, 2000 and the IT amendment act, 2008 had clearly laid the provisions of investigation mechanism up to some extent only. The cyber crime convictions in India are very low due to the fact that there is a serious lacuna that exists on the part of investigation agencies in providing the scientific evidence and lack of knowledge by the investigation agencies with regard to cyber crime and cyber laws. Today, with the advent of modern technology, cyber crimes have become more prevalent, complex and the cyber criminals had turned more sophisticated and their modus operandi is no way comparison to the existing traditional methods of investigation. The tools of information technology provides greater chances for the offenders in order to commit traditional and as well as cyber crimes which includes cyber terrorism also.

The crimes related in information technology like attacks against the digital security of the crucial infrastructure and logistics like banking, mobile communication and other emergency services. Generally the cyber crimes are committed through the available network of computers in the form of internet and sometimes it may be across the national boarders with effects individuals and as well as other nations in terms of economy and national security. Cyber crime investigation mechanism requires the requisite technical expertise for investigating the cyber crime by the concerned investigation officers. The collection of evidence is very crucial and it is technical or scientific by its nature and it requires personal skills and experience.

V. METHODS AND PROCESS OF INVESTIGATION UNDER THE IT ACT, 2000

The nature of the IT Act, 2000 and the IT Amendment Act, 2008 is said to be more business law rather than the criminal law. This makes the Indian investigation authorities to follow the provisions of conventional criminal laws in the process of investigating the cyber crimes. The IT act is of procedural and substantive nature. The various provisions under this said act provides the nature of the offences and the penal provisions as well as the investigating procedure of the cyber crime. Sections 78 and 80 deals with the investigation power along with the search and seizure and procedures for the arrest of the accused person.

The prevailing provisions under the IT act do not have the sufficient perimeter in order to meet the requirements of cyber law investigation and hence the CrPC and IPC are also amended in order to bring the cyber crime
under the ambit of cyber law and they are subjected to conventional crime. The various provisions of IT act, 2000 foresee the special procedure for cyber crime investigation but all the existing procedural laws of conventional nature are applicable to the investigation process. The IT amendment act, 2008 clearly says that a police officer not below the rank of inspector shall investigate any offence under this act.

In the modern day technological world the criminal investigation procedures require drastic changes in order to handle the wayward computer users in an effective and efficient manner. The investigation agencies are facing many problems in the collection of the related and relevant evidence from the storage media of the computer and the digital communication system. It demands the availability of well equipped and trained investigation force that can operate and coordinate at international and national level.

There is every need on part of the forensic support platform in order to reequip themselves with better procedures and logistics for aiding the investigating agencies in the needy times of cyber crime scenario. There is every need for the major changes in the outlook of the judiciary also. If the necessary steps were not taken properly and immediately, the modern technology can soon disrupt and wreck the criminal justice system and it will turn the whole exercise pointless.

VI. CHALLENGES AND PROBLEMS OF CYBER CRIME INVESTIGATION

As per the changing needs in the society in terms of crime aspects, criminal law has to be modified as per the changing situations and needs because crime is not a static concept. Unfortunately the Indian criminal investigation and policing system is not modified and it was logged in the traditional ways of gathering information and extracting the confessions from the crime suspects. It can be said that the Indian police force has not tuned itself to modern ways of investigation methods, gathering of scientific evidence and to present the water tight cases in the criminal courts. This made the existing gaps to continue in between the information and report of crime stage to arresting the criminals and finally for the successful prosecution with regard to the accused person in the crime. In the case of cyber crimes in India, investigation modes and methods are no way synchronized to the changing circumstances and modus operandi of the criminals in cyber crimes.

With regard to the existing problems of investigation procedures under the cyber crime, the policing system from every state differs with each other across the nation and this leaves wider corridor for the criminals to run freely by avoiding arrest and penal provisions under the law. The lack of technical education among the police personnel also hampers the scientific procedure of investigation methodologies in the cyber crimes. The training pedagogies are to be matched with the requisite technical background and scientific approach towards the effective investigation methods of cyber crimes. Another limitation in this process is lack of access to data from national crime records bureau to investigation agencies at all levels. Added to the problematic platform of handling cyber crimes is the lack of manpower factor and technological logistics support at various stages of investigation process in terms of cyber crimes. The formulation of National Cyber Security Policy (NCSP) may resolve the existing problems in future.

VII. CONCLUSION AND SUGGESTIONS

From the findings and observations of this present research study, it may be concluded that the police department is handicapped in undertaking the effective procedures of investigation due to the lack of modern digital logistics like digital video and audio tracking devices and there is a severe shortage of the availability of forensic lab facilities and services that render the necessary assistance at the appropriate time for the investigating agency.

It was further observed that there is a severe dearth of cyber experts and IT technocrats those attached to investigating agencies and this makes the investigating authorities to rely heavily on oral evidence in the place of circumstantial or scientific evidence. The present scenario demands the promptness by the investigating agency in terms of devoting the time and effort for examining the witnesses and recording their statements. Moreover the information and the statements related to cyber crime are not being seriously attended and examined by the investigating authorities and there is no seriousness involved in framing the charge sheets with requisite technical or scientific evidence in relation to the crimes under the cyber law.

The existing problems in the detection and investigation process of cyber crime poses a severe threat on part of the police department and this events will certainly provide the sufficient room for the criminals to evade and
escape the penal provisions of law. Keeping these things in view, the IT act 2000 and the IT amendment Act, 2008 has changed the investigative provisions to a certain extent and yet there exists wider technical gaps in making the tight cases under cyber law. The above mentioned cyber laws has drastically transformed the basic nature of the Indian cyber law. Though there exists new provisions covering the investigative procedures under cyber laws, many new milestones in terms of technology and digital process have to be reached by the investigating agencies and this requires appropriate training and logistic support for the cyber law implementing authorities and cyber law regulatory bodies.

REFERENCES
10. The IT Amendment Act, 2008