CYBER CRIMES AND CRIMINAL JUSTICE SYSTEM IN INDIA

Dr. Shiv Raman*

INTRODUCTION

The Criminal Justice System is an integral part of strong and developed democratic system of India. After the evolution of civilization, we felt the requirement of a developed administration of the Criminal Justice System. In due course, many institutions have been established for the administration of an impartial Judicial System. A strong Criminal Justice System has four constituent elements:

1. Police and other agencies, as Investigative Units.
2. Prosecution, to prosecute in Court of law.
3. Impartial, Independent and Transparent Courts, for adjudication of disputes.
4. The Prison and Correctional Institutions.

In the present Digital World, new technologies and new inventions are taking place and many more technological developments are under process. Computer-based technology is used for enhancing the modern life everywhere including education, commercial sectors and Govt. organizations, etc. It ensures the efficiency and productivity. On the other side, *'the excessive dependence'* over technology is the root cause of Cyber Criminals for committing unlawful and unethical activities with the use of Computers and the Internet.

The collection and compilation of Digital Evidence from Computer and IT-based devices is the most challenging job for all investigating agencies in India. The investigation and collection of evidence from Computers require expertise, special knowledge and skill, which is lacking in most technical personnel of our country.[1]

Nowadays India has developed as a favorite nucleus for Cyber Criminals, especially hackers and other malevolent users, who use the Internet as a tool for Cyber Crimes. The rising trend of Cyber Crimes includes Cyber-spamming, Hacking, Cyber Stacking including theft, phishing, etc. Time has come for the Indian Police to overhaul and reform investigating methodology for a successful prosecution of Cyber cases in country. Indian traditional system

* *Asst. Professor* @ Amity Law School, Amity University Haryana (Gurugram)

[1] Vanthi J. Jayaprasana S, *A study of Cyber Crimes in the digital world, International Journal on recent & Innovation trends in computing & communication*, 2014 Sep. 2(9): pp.1-4.

of policing and criminal investigation is out dated, our extracting, gathering information and obtaining confession by beating. The Police force is still untrained in modern methods of criminal investigation, which needs special skills for managing and operating highly sophisticated technologies.

For the investigation of Cyber Crimes, jurisdiction remains the highly controversial issue for the maintainability of criminal or civil prosecution. Due to the development of cyberspace, the territorial boundaries seem to have disappeared but we still depend on Section 16 of Criminal Procedure Code, 1973 and Section 2 of Indian Penal Code, 1860.

The laws relating to computer-related crimes include Cyber Crimes, E-commerce, Copy Rights, IPR rights, Freedom of Expression & Privacy related rights, both in the physical & virtual world. In the 'Cyber Criminal Justice System', the investigation into the Cyber Crimes and collection of Evidences is worthless unless the prosecution secures the conviction of criminals including Computer/ Internet-related or involved crimes. The discovery of Digital Evidence is not an easy task. All or some of the evidences may be in E- form without 'any fact-filled story' or human Evidences. There the Computer Forensics Examiner will have a vital role. The Cyber Forensics Examiner must be able to convince the court and the reliability of electronic Evidence.

THE INDIAN CYBER CRIMINAL JUSTICE SYSTEM

India has an established Criminal Justice System inclusive of Indian Penal Code, 1860, Code of Criminal Procedure, 1973, Indian Evidence Act, 1872 and other penal laws & provisions in other laws. The registered Cyber Crimes in India are of various categories i.e.; under Information Technology (IT) Act, 2000, Indian Penal Code, 1860 and other State levels Legislations (SLL).

The Legal Regulations for handling Cyber Crime cases

In India, the Ministry of Home Affairs has advised the Union Territories and State Governments to tackle Cyber Crime cases by establishing- Cyber Cells equipped with the latest modern technical structures. These are:

- Cyber Police Stations;
- Experienced/trained Cyber Analysts/ Experts for Cyber Crime detections and filing of cases.

- Expert Cyber Prosecutors and
- Govt. of India has implemented a plan for the expansion of Cyber- Forensics tools and establishing Cyber- Forensics labs.

Cyber Crimes and preventive measures to deal with Cyber Crimes

Before dealing with agencies, steps and processes of Cyber Crime's Investigation and Cyber-Forensics, it is necessary to know the preventive measures to deal with Cyber related or involved Crimes. The Govt. of India's Department of Electronics & Information Technology, Ministry of Communications & Information Technology has established CERT-IN(Indian Computer Emergency Response Team) and issues advisories regularly for the common use of:

- Mobile Phone & Data Security;
- Desktop Security;
- Broadband Internet Security;
- USB and Storage devices Security and
- Secure use of Debit/Credit Card and phishing of Attacks, which are disseminated through the portals.

Through the under mentioned web portals or with the assistance of other portals may be developed in this behalf:

- www.secureyourelectronics.inwww.secureyourpc.in
- www.cert-in-org.in[2]

Indian Computer Emergency Response Team (CERT-IN)

Whenever an incident relating to Computer Security occurs then we can report to the CERT-IN, the National Agency. Section 70B of Information Technology Act, 2000 and IT Amendment Act, 2008 has designated CERT-IN to serve as with the following objectives in the fields of:

A. Dissemination and Analysis of information on Cyber incidents

- To alert and forecast of Cyber Security incidents;

[2] Available at: http://infosecawareness.in/cybercrimes-cells-in-india

- Urgent and Emergency measures for handling incidents of Cyber Security;
- Coordination with Cyber incident response activities;
- Issue Advisories, Guidelines, vulnerably- Notes and White Papers relating to information security, practice, prevention, procedure reporting and response to cyber incidents.

B. Matters to be reported to CERT-IN

The System Administrators and users can report Computer Security incidents and vulnerabilities to CERT-IN. The CERT-IN provides technical assistance for:

- Denial and disruption of services;
- Storage and processing of data by unauthorized use of Computer system;
- Gain or attempts to gain unauthorized access to a system in India and
- Issues related to Electronic Mail Security, Mail Bombing, Spamming, etc.[3]

C. The procedure of filing report to CERT-IN

The Cyber Victims can report Cyber related incidents by filling up online form, Electronic Mail, by Fax or Telephone hotline or by postal services[4]. In fact, the most appropriate way for reporting a Cyber Crime is to follow the procedure enshrined in Sec. 69A[5] of IT Act, 2000 read with Procedure and Safeguards for Blocking for Access of Information by Public Rules, 2009 of IT Act, 2000. It gives the power to Central Govt. to issue directions for blocking public access of any information through any Computer resource and Sec. 79(3) (b)[6] of the said Act exempts the liability of intermediary[7] in certain cases about particular E-record including Telecom Service, Network Service, Internet Service, Web- Hosting Service, Search Engines, E- Payment Sites, E-Auction Sites, Cybercafés, and E- market places.

D. Cyber Police to deal with Cyber Crimes in India

Another way for the protection and detection of Cyber Crimes in India is- Crime and

[3] How to Report Cyber Crime in Indian territory, Ompal, Tarun Pandey, Basir Alam, Ministry of Electronics & Information Technology, Dept. of Computer engineering, Faculty of Engineering & Technology Jamia Millia Islami, New Delhi (India), International Journal of Science Technology & Management, Vol. No. 6, Issue No. 04. April 2017. www.ijstm.com ,ISSN (O) 2394-1537 and ISSN (P) 2394-1529.
[4] Email- info@cert-in.org.in, Phone: +91-11-24368572, Fax: +91-11-24368546.
[5] Sec. 69A, IT Act
[6] Sec. 79, IT Act
[7] Sec. 2(1)(w)

Criminal Tracking System, which was approved by the Central Govt. in 2009 under the National E-Governance project however, by using IT-enabled tracking and Crime detection system. But unfortunately, until today it is not completed by all the States in India. The Investigation process of such crimes is often not exactly similar to other crimes.

E. The Process of Cyber Investigation

Cyber Crimes usually transgress geographical hurdles. Cyber Crime is a fast-growing meadows of crimes. Cyber criminals are exploiting the speed barriers and anonymity of the internet for commission of different types of criminal activities. No border, virtual or physical, can cause serious harm and rise real threats to worldwide victims other than Cyber Crimes.[8] To deal with the issue of Cyber Crimes, the Criminal Investigation Department (CID) established, Cyber Crime Cells (CCC). The IT Act, 2000 makes it clear that- *'whenever a Cybercrime has been committed, it has a global jurisdiction and hence a complaint can be filed at any Cyber cell'*.[9] Further, to combat Cyber Crimes, the CBI (Central Bureau of Investigation) has created specialized units:

- Cyber Crimes Investigation Cell (CCIC);
- Cyber Crimes Research & Development Unit (CCRDU);
- Cyber Forensics Laboratory (CFL);
- Network Monitoring Centre;[10]

F. Cyber Crimes Investigation Cell (CCIC)

The CCIC was established in Sep. 1999. It has jurisdiction all over India. It acts as a part of economic offense. CCIC is empowered to investigate all the Cyber Crimes under IT Act, 2000. It also acts round the clock as the Nodal Point of contact with Interpol to report Cyber Crimes in India. The CCIC of India is also a member of the 'Cyber Crimes Technology Information Network System, Japan'.

G. Cyber Crimes Research and Development Unit (CCRDU)

It is the responsibility of CCRDU to track the development and changes, which take place in

[8] IJSTM.com, Vol. No. 6, Issue No. 04, April 2017.
[9] How to Register Cyber Crime Complaint with Cyber Cell of Police - online Complaint procedure- by Ramanuj, May 25, 2014.
[10] Available at: https://www.yumpu.com/en/document/view/28923514/crime-manual-2005-full-in-pdf-central-bureau-of-investigation

ever-changing area. It has the following functions:

- To ensure cooperation and coordination with State Police Forces;
- To collect and compile the data of reported Cybercrime cases to Police for investigation;
- To coordinate with software experts in the identification of areas, which require the attention of State Police and
- To obtain the information of Cyber Crimes cases reported in other countries and prepare a monthly Cyber Crime digest.

H. Cyber Forensics Laboratories (CFL)

Cyber Forensic Laboratories are one of the primary wings of Cyber Investigation to provide investigative services in Computer Forensics (Digital Forensics), Forensic Data Revival, and Digital Evidence Detection. CFL can analyze the forensic data and recover Digital Evidence while maintaining the veracity of the electronic Evidence for detection and trial. The basic functions of the Cyber Forensics Laboratory (CFL) are to:

- Ascertain and scientifically Scientific analysis of Digital Foot- Print;
- Provide scientific analysis in support of the Crimes Investigation by Law Enforcement Agencies and CBI;
- Assist on-site for Computer seizure and search, on request;
- Provide consultation services for activities or investigations, where media analysis is probably occurring;
- Provide expert testimony and
- Provide adequate research and development in Cyber Forensics.

The information so collected and analysis thereof can be used as evidence in s Court of Law.

I. Cybercrime Investigations

Cyber Crimes can be defined as- *'a crime in which a computer is the object of the crime or is used as a tool for the commission of cyber offense'.*

Cyber Crime can also be defined as – *'a crime where Computer is the target or a crime committed through the use of a Computer'.* There is a long list of identified Cyber Crimes. All the crimes have different legal punishments provided in Information Technology Laws.

The Cyber Crime Investigation is almost similar to the investigation of regular crimes, except

that the Cyber investigators use Computers as a tool of Investigation and data as sources of evidence. The investigation of Cyber Crime has consequently become a highly specialized professional field.[11]

J. Relevant Legal Provision in Cr.Pc, 1973 for Cyber Investigation

The Code of Criminal Procedure, 1973 contains various legal provisions regarding the investigation of Criminal offenses which are also applicable to investigation of Cyber Crimes offenses. Here below is a list of those legal provisions:

- Power of Police to arrest without warrant-Sec. 41
- Power to search place entered by person sought to be arrested- Sec. 47
- Issuing Summons to produce document or other things- Sec. 91
- Grounds when search warrant may be issued- Sec. 93
- Power to search place suspected to contain stolen property, forged documents, etc.- Sec. 94
- Power of Police Officer to seize certain property- Sec. 102
- Power of Police to arrest to prevent commission of cognizable offenses- Sec. 151
- Procedure to be adopted for investigation- Sec. 157
- Investigation Report to be submitted to magistrate- Sec. 158
- Police Officer's power to require attendance of witnesses- Sec. 160
- Power of Police for examination of witnesses- Sec. 161
- Power of search by Police officer- Sec. 165
- When Officer Incharge of Police Station may require another to issue search warrant- Sec. 166
- Letter of request to the competent authority for investigation in a country or place outside India- Sec. 166A
- Procedure when investigation cannot be completed with in twenty-four hours- Sec. 167
- Police Diary of proceedings in investigation- Sec. 172
- Report of Police Officer on completion of investigation- Sec. 173
- Power to summon persons- Sec. 175[12]

[11] Available at: https://www.yumpu.com/en/document/view/28923514/crime-manual-2005-full-in-pdf-central-bureau-of-investigation

[12] Bare Act, The Code of Criminal Procedure, 1973.

K. Determination of Cyber Crime Jurisdiction: Provisions in Cr. Pc, 1973 and IT Act, 2000:

The word jurisdiction derives its origin from the Latin word '*jus, Juris* and *diare'* meaning thereby *'Law' and 'Speak'*. Jurisdiction and competency of the Court is the most important aspect of every Criminal Justice System. Every jurisdictional error and incompetency of Court is always an error of law of court. Every Court has an inherent right to decide these things. A decision without jurisdiction and incompetency is a *coram non judice* and *denial of justice*. Jurisdiction is the legal and statutory right of the court to hear and decide a case.

Today cyber-world has no geological precincts. It can establish instant remote communications with anyone who can have access to the computer or the Internet. Generally, a web-user is unaware of the source and the network and servers/routes exactly from where the information on a site is being accessed. Jurisdictional issues are of primary importance in Cyber-world. World Wide Web (www) does not make a clear geographical and jurisdiction border. The web user though physically is one place but maybe in the jurisdiction of another country virtually or technologically. Even a single Cyber /web- transaction may engross the laws of at least three jurisdictions. Below is the list of legal provisions enumerated in Code of Criminal Procedure Code, 1973 and Information Technology Act, 2000 which deal with the determination of jurisdiction for Investigation of Cyber Offences:

- Place of Trail/ Inquiry where the offense was committed- Sec. 177;
- If the offense committed in more than one jurisdiction- any of the relevant jurisdictions- Sec. 178;
- Where the accused is found to possess the property obtained in theft, extortion or stolen property- Sec. 181;
- Offenses committed by letters, massages- where send or received- Sec. 182;
- Offenses committed outside India by an Indian citizen, on aircraft registered in India, tried as if the offense committed in India with the prior sanction of Central Govt.- Sec. 188;
- Period of limitation to take cognizance- Sec. 468;
- Confiscation of any Computer or accessory liable to be confiscated if used for commission of offense- Sec. 77 r/w Sec. 81 of IT Act, 2000;
- Compensation, penalty, confiscation not to interfere with other remedies under statutes;

- Compounding of offenses, where the sentence is below 3 years Sec. 77A of IT Act, 2000;
- Offense with 3-years punishment are bailable- Sec. 77B;
- Power to the investigate is given to Inspector and above the rank of Inspector-Sec. 78 of IT Act, 2000 and
- Inspection provision- to be consistent with Sec. 80 of IT Act, 2000, which gives the power of Police Inspector/ Officer to search and arrest, without warrant any person who has committed, is committing or about to commit any offense under IT Act, 2000- Sec. 80.

L. Rules in CBI Manual, 2005 for Investigation of Cyber Crimes, Chapter 18

To deal with Cyber Crimes effectively, the Central Bureau of Investigation (CBI) is empowered with its other Units under Chapter-18 of the CBI Manual, 2005, The important provision in this regard are:

- Cartridges or disk- can be used for the restoration of copies of files from Computer, useful for investigation.
- Labeling of Evidence- Label cables, where they are plug-in, disks, the various other parts of a computer and to write /protect disks.
- Dismantle the hardware with screwdrivers other tools for seizure.
- Use of Gloves- Often latest prints can be taken from disks or other storage hardware or media.
- Material needed for packing- Tapes, boxes, rubber bands, bubble wrap and if he does not have access to anti-static wrap then papers, bags can be used.
- Recording Equipment- to video graph and taking photographs of the crime scene
- Custody of report sheets and other paper for inventories and seize Evidence.[13]

CONCLUSION

As in depth analysis of *cyber-crimes* and laws related thereto reveal acquainted various problems being countenanced by India, is Criminal Justice System while implementing and protecting Cyber world from the ultra-tech Cybercriminals. Even though Cyber Crime is

[13] Available at: https://www.yumpu.com/en/document/view/28923514/crime-manual-2005-full-in-pdf-central-bureau-of-investigation

global issue of international concern, but still- every country has its different definition of 'Cyber-crime'. The common consensus of a harmonious definition is an illusion to imagine. This poses severe issues while implementing Cyber Laws and policies and provides ample opportunities for cyber perpetrators to get away from the judicial process and punishment. Further, the misuse of powers even by Police and cyber authorities cannot be ruled out. Simultaneously it is also required to be considered that the hazards of the 'virtual offenses are increasing day by day. So, Cyber Law Enforcement Agencies are required to give the Police ample powers to apprehend offenders for commission of these crimes.