VOL. 2 ISSUE 3
DROIT PENALE: INDIAN LAW JOURNAL ON CRIME & CRIMINOLOGY
ISSN: 2456-7280

CYBER CRIME INVESTIGATION IN INDIA

-Manoj Singh[1]

ABSTRACT

Cyber crime is unlawful acts wherein the computer is either a tool or target or both. Cyber crime has a widespread problem in view of the internet in everyday life. The targets of cybercrime include any device, which can access the internet like a computer, Smartphone or laptop, and any activity that is conducted using information technology. Cyber crimes can be divided in three categories 1.Cyber crime against person for example harassment, obscenity, and cyber stalking etc.2. Cyber crime against property for example illegal online fund transfer, online cheating and fraud etc. 3. Cyber crime against government or nations for example cracking government maintained website and cyber terrorism etc. Cyber crime investigation is the collecting, analyzing and investigation of electronic evidence and cyber trails. All the cyber crimes are not covered under Information Technology Act, 2000, many cyber crimes are covered Under Indian Penal Code.1860 which are triable according to the provisions of Criminal Procedure Code, 1973. The Information Technology Act, 2000 provides a legal framework to aid investigation, search and seizure required by cybercrime. Since Information Technology Act, 2000 has overriding effect, the provisions of Information Technology Act, 2000 will prevail on Criminal Procedure Code, 1973 in case of conflict. Day by day investigation of cyber crime will be complex because cyber criminals are also becoming aware of new technologies. Cyber crime police stations separately should be established district wise so that such crimes can be investigated without doing any delay because evidence in cyber crime can be deleted easily.

Key words; Cyber crime, cyber stalking, investigation, Cyber crime investigation.

[1] Assistant Professor, Faculty of Juridical Sciences, Rama University, Kanpur, Uttar Pradesh.

Cyber Crime;

Cyber crime is a new branch of crime which has not been defined in Indian laws including the Information Technology Act; 2000.A cyber crime is any crime committed using a computer.[2]C.B.I. Manual defines cyber crime as;

1. Crimes committed by using computer as a mean including conventional crimes

2. Crimes in which computers are targets.

A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both".[3]

Cyber crimes are the crimes committed with respect to the cyber world or any component thereof. However, cyber crime may also be viewed as the acts which have been declared as such under any cyber law in force in a particular legal system.[4]

These days menace of cyber crime is growing, besides traditional crime like identity theft and including people to pay for imaginary services and non-existent goods, a new ingenious variant to it now came from different kind of individual and group.[5]

Cyber crime has a widespread problem in view of the internet in everyday life. The targets of cybercrime include any device, which can access the internet like a computer, Smartphone or laptop, and any activity that is conducted using information technology.[6]

A cyber crime invites the application of not only the cyber-crime specific legislation, which Information Technology Act, 2000, but also general criminal legislation like Indian Penal Code, 1860.Other laws will be applicable depending on the nature of the crime. It does not need an expert knowledge of computer.

[2] ANIRUDH RASTOGI, CYBER LAW 81(2014).
[3] Justice K.N.Bashaina, Seminar Detection *Of Cyber Crime And Investigation* (Apr., 11, 2018, 12:56PM), http://www.tnsja.tn.nic.in/article/Cyber%20Crime%20by%20KNBJ.pdf.
[4] Dr. J.P. MISHRA, AN INTRODUCTION TO CYBER LAW 17(2nd ed. 2014.)
[5] THAKUR SHAILENDRA NATYH, WHITE COLLAR CRIMES X-POSED 140 (2010)
[6] ANIRUDH RASTOGI, CYBER LAW 82(2014).

Classification of Cyber Crime;

Cyber crimes can be divided in three categories

1. Cyber crime against person for example harassment, obscenity, cyber stalking etc.

2. Cyber crime against property for example illegal online fund transfer, online cheating and fraud etc.

3. Cyber crime against government or nations for example cracking government maintained website and cyber terrorism etc.

Cyber Crime Investigation;

Cyber crime investigation is the collecting, analyzing and investigation of electronic evidence and cyber trails.[7] This digital evidence and cyber trail may be found in computer hard discs, cell phones, CDs, DVDs, floppies, computer networks, the internet etc.electronic evidence and cyber trails can be hidden in pictures, encrypted files, deleted files, formatted hard disks, deleted e-mails, chat transcripts etc.electronic evidence and cyber trails can relate to online banking, frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabogate,phising attacks-mail hijacking, denial or service,hacking,diverce ceses,murder cases, organized crime, terrorist operations,defamation,pornography,extortation,smuggling etc.[8]

Evidence being intangible in cyber crime investigation is always too much complex. Criminal are one step ahead in the sense that they create technology or come up with technique to perpetrate a particular crime and the law enforcers then counter such techniques or technologies.[9] Cyber crime being technology driven evolves continuously and ingeniously making it difficult for investigators to cope up with changes.[10]Cyber crime investigation is very tough job as it requires knowledge of computer sciences, forensic science, Criminal .Procedure College, 1973, Indian Penal Code, 1860 including Indian Evidence Act, 1872

[7] FABIO GIACOMINI & M.HASAN JAIDI, ELECTRONIC EVIDENCE 526(2012).
[8] Ibid.
[9] Justice K.N.Bashaina,Seminar Detection *Of Cyber Crime And Investigation* (April 11.,2018,12:56PM), http://www.tnsja.tn.nic.in/article/Cyber%20Crime%20by%20KNBJ.pdf.
[10] Ibid.

Statutory Provisions Regarding Cyber Crime Investigation

Cyber crime and Indian Penal Code, 1860;

All the cyber crimes are not covered under Information Technology Act, 2000, many cyber crimes are covered Under Indian Penal Code,1860 which are triable according to the provisions of Criminal Procedure Code, 1973.Ss.172 (failing to produce electronic document in court),175 (failing to produce electronic document to a public servant),192(making false entries in electronic document),204(destroying a document in electronic format or making it),292(transmitting obscene e-mail/SMS/MMS)383(web jacking),406 (criminal breach of trust),420(cyber frauds),466(forgery),465(forgery of electronic records),471(making use of forge record),509(sending an e-mail outraging the modesty),499(sending defamatory message by e-mail),506(sending threatening message by e-mail) are cyber crimes covered under Indian Penal Code,1860.

Cyber crime and Criminal Procedure Code;

S.2 (h) Of The Criminal Procedure Code, 1973 says "investigation includes all the proceeding under this code for the collection of evidence conducted by a police officer or by any person (other than a magistrate) who is authorized by a magistrate in this behalf." It means investigation is a process of collecting evidence which is made by either a police officer or a person authorized by magistrate. It includes proceeding to location of crime, deputing a subordinate to ascertain facts, discovery and arrest of suspected offender and collection of evidence and also recording statement of relevant witnesses. Search of premises and seizures of items may also be done unless otherwise provided in any enactment; all offences are to be investigated according to the provisions of Criminal. Procedure Code, 1973.[11]

The Information Technology Act, 2000 provides a legal framework to aid investigation, search and seizure required by cybercrime. Since The Information Technology Act, 2000 has overriding effect, the provisions of The Information Technology Act, 2000 will prevail on Cr.P.C.in case of conflict. Central Bureau Of Investigation and Data Security Council Of India have issued

[11] FABIO GIACOMINI & M.HASAN JAIDI, ELECTRONIC EVIDENCE 547(2012).

guidelines with respect to investigation, search and seizure required by cybercrime.[12]The DSTI issued a 'Cybercrime Investigation Manual' in 2011, which standardizes the operating procedures for cybercrime investigation and is proposed to be distributed to police stations throughout the country.

Cyber Crime and Information Technology Act;

Power to investigate a cyber crime;

Section 78 Of The Information Technology Act, 2000 deals about power to investigate a cyber crime which says that notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Power of Police Officer for enter, search and arrest;

Power of Police Officer for enter, search and arrest is under Section 80 of the Information Technology Act, 2000 which runs as under;

(1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 any police officer, not below the rank of a Deputy Superintendent of Police or any other officer of the Central Government or a State Government authorized by the Central Government in this behalf may enter any public place and search and the Central Government in this behalf may enter any public place and search and arrest without warrant any person found therein who is reasonably suspected of having committed or of committing or of being about to commit any offence under this Act.

Explanation:- For the purposes of this sub-section, the expression "public place" includes any public conveyance, any hotel, any shop or any other place intended for use by, or accessible to the public.

[12] Dr. J.P. MISHRA, AN INTRODUCTION TO CYBER LAW 17(2nd ed. 2014).

(2) Where any person is arrested under sub-section (1) by an officer other than a police officer, such officer shall, without unnecessary delay, take or sent the person arrest before a magistrate having jurisdiction in the case or before the officer-in-charge of a police station.

(3) The provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

Provisions of criminal procedure code, 1973 in relation to entry, search and or arrest

S.80(3) of The Information Technology Act, 2000 provisions of the Code of Criminal Procedure, 1973 shall, subject to the provisions of this section, apply, so far as may be, in relation to any entry, search or arrest, made under this section.

The powers given under this section are without any restrictions and are likely to be misused by the police authorities.[13]

Penalty for failure to furnish information, return, etc.-

Section 44 of the Information Technology Act, 2000 provides for Penalty for failure to furnish information, return, etc which says "If any person who is required under this Act or any rules or regulations made there under to-

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each 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 return or 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 such failure continues;

[13] ANIRUDH RASTOGI, CYBER LAW 211(2014).

(c) maintain books of account or records fail to maintain the same, he shall be liable to a penalty no exceeding ten thousand rupees for every day during which the failure continues".

Power to adjudicate;

Section 46 of the Information Technology Act, 2000 is about power to adjudicate which is as under;

"(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made there under the Central Government shall, subject to the provisions of sub section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government .

(2) The adjudicating officer shall, after giving the person referred to in sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3) No person shall be appointed as an adjudicating officer unless he possesses such experience in the filed of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4) Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5) Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under sub-section (2) of section (2) of section 58, and-

(a) all proceedings before it shall be deemed to be judicial proceedings within the meaning of section 193 and 228 of the Indian Penal Code,1860 (45 of 1860);

(b) shall be deemed to be a civil court for the purpose of section 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974)."

Punishment for publishing or transmitting obscene material in electronic form;

Section 67 of The Information Technology Act, 2000 provides for Punishment for publishing or transmitting obscene material in electronic form.- Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to two three years and with fine which may extend to five lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Powers to issue directions for interception or monitoring or decryption of any information through any computer resource;

Section 69 of The Information Technology Act, 2000 provides for Powers to issue directions for interception or monitoring or decryption of any information through any computer resource which speaks " (1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.
(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in charge of the computer resource shall, when

called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
(b) intercept or monitor or decrypt the information, as the case may be; or

(c) Provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine."

In case People's Union of Civil Liberties vs Union of India[14] Constitutional validity of interception was by the government was challenged in Supreme Court in which our apex court held that" On the occurrence of any public emergency, or in the interest of public safety, the Central Government or a State Government or any Officer specially authorized in this behalf by the Central Govt. or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order."

Power to issue directions for blocking for public access of any information through any computer resource;

Section 69A of The Information Technology Act, 2000 is related to Power to issue directions for blocking for public access of any information through any computer resource which says " (1) Where the Central Government or any of its officer specially authorized by it in this behalf is

[14] (1997)1 SCC 301.

satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-sections (2) for reasons to be recorded in writing, by order direct any agency of the Government or intermediary to block access by the public or cause to be blocked for access by public any information generated, transmitted, received, stored or hosted in any computer resource.
(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out shall be such as may be prescribed.
(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine."

Power of central government to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security;

Section 69B The Information Technology Act, 2000 enables Central Government to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security. This is as under;

" (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.
(2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating, transmitting, receiving or storing such traffic data or information.
(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.
(4) Any intermediary who intentionally or knowingly contravenes the provisions of subsection

(2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section,
(i) "Computer Contaminant" shall have the meaning assigned to it in section 43
(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information."

Confiscation;

Section 76 The Information Technology Act, 2000 deals about Confiscation which speaks " Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit."

Provision regarding power to investigate contraventions;

Section 28 of The Information Technology Act, 2000 provides provision regarding power to investigate contraventions which says "(1) The Controller or any officer authorized by him in this behalf shall take up for investigation any contravention of the provisions of this Act, rules or regulations made there under.

(2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act."

The controller's power under this section is only for contraventions occurred in India however, if sub section (1) of this section read with section 75 of the Act. It gives power to the controller to investigate contraventions that occurred outside India also."[15]

Access to computers and data;

Section 29 The Information Technology Act, 2000 deals about Access to computers and data which runs as under

" (1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. (2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary."

Penalty for misrepresentation.-

Section 71 of The Information Technology Act, 2000 declares "Whoever makes any misrepresentation, to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a terms which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

[15] ANIRUDH RASTOGI; CYBER LAW 211(2014).

Breach of confidentiality and privacy;

Section 72 of the Information Technology Act, 2000 states **"**Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both"

Penalty for publishing Digital Signature Certificate false in certain particulars;

Section 73 of the Information Technology Act, 2000 **says** "(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended, unless such publication is for the purposes of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both".

Publication for fraudulent purpose;

Section 74 of the Information Technology Act, 2000 declares "whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both".

Act to apply for offence or contravention committed outside India;

Section 75 of the Information Technology Act, 2000 states **"(**1) Subject to the provision of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting located in India".

Penalties and confiscation not to interfere with other punishments;

Section 77 of the Information Technology Act, 2000 says "No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force".

Network service providers not to be liable in certain cases;

Section 79 of the Information Technology Act, 2000 declares "For the removal of doubts, it is hereby declared that no person providing any service as a network service provider shall be liable under this Act, rules or regulations made there under for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence for contravention."

Compounding of Offences;

Section 77A The Information Technology Act, 2000 deals about Compounding of Offences under the Act, which speaks

" (1) A Court of competent jurisdiction may compound offences other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under this Act.

Provided that the Court shall not compound such offence where the accused is by reason of his previous conviction, liable to either enhanced punishment or to a punishment of a different kind.

Provided further that the Court shall not compound any offence where such offence affects the socio-economic conditions of the country or has been committed against a child below the age of 18 years or a woman.

(2) The person accused of an offence under this act may file an application for compounding in the court in which offence is pending for trial and the provisions of section 265 B and 265C of Code of Criminal Procedures, 1973 shall apply."

Section 77B of The Information Technology Act, 2000 declares Offences with three years imprisonment to be cognizable which says "Notwithstanding anything contained in Criminal Procedure Code 1973, the offence punishable with imprisonment of three years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable."

To prove the Cyber Crime-evidence require[16];

- Attachments and copies of e-mail with header detail (with IP address)
- Details of IP address with intermediary.
- Intermediary (Service Provider) Server and Routers Log.
- Recording of CCTV and Video Camera.
- Electronic/Digital signature.

Day by day investigation of cyber crime will be complex because cyber criminals are also becoming aware of new technologies. Cyber crime police stations separately should be established district wise so that such crimes can be investigated without doing any delay

[16] FABIO GIACOMINI & M.HASAN JAIDI, ELECTRONIC EVIDENCE 554(2012).

because evidence in cyber crime can be deleted easily. Law relating to cyber crime exists in India but it is very much complicated it should be made simpler. Cyber forensic experts has important role in cyber crime investigation therefore special institute for preparing cyber forensic expert should be opened where they can be prepared. Public awareness is must for combating against cyber crime. Half of the problems relating to cyber crime can be reduced by public awareness.