INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

CYBER LAW vis-à-vis PROCEDURAL LAW: A CRITICAL ANALYSIS

***PIYUSH PATEL**

ABSTRACT

The need for the administration of Criminal Justice has been felt by humanity since the dawn of civilization. A number of institutions have been developed in course of time to administer justice to the people. In the operative part of the system of Criminal Justice there are four distinct components or constituent elements, namely, the Police, that is the investigative agency; the Prosecution, that is the agency to pursue a case in a court of law on behalf of the society; the courts, that is the Judiciary to try and decide about the guilt or innocence of a certain person and the Prison and correctional institutions. The problems associated with cybercrimes are not limited to formulating substantive criminal laws. Also these problems are not restricted to prosecution of cybercrimes alone but extend too many other fields of criminal investigation.

INTRODUCTION

The fundamental basis for Criminal Justice System is the law of the land. The very process of law in a democratic society ensures a measure of public sanction for law through the consent expressed by their elected representatives. Our cyber investigations experts reflect our multidisciplinary team approach to problem solving.[1433] The entire criminal justice system in our country therefore revolves round the Criminal Law enacted by the Union Parliament and the State Legislatures.[1434]

After laws are made by the legislative institutions their enforcement is taken up by various agencies set up for the purpose by the Government. Police comes at this stage as the primary law enforcement agency available to the State. Enforcement by Police is primarily an exercise of taking due notice of the infraction of laws as soon as it occurs and ascertaining the connected facts thereof including the identity of the offender. This particular task in the system of Criminal Justice is known as Investigation.

*Student, Faculty of Law, University of Lucknow, UP.

[1433] http://www.kroll.com/cyber-security/cyber-crime-investigations

[1434] http://www.angelfire.com/theforce/npcreport/Vol2Chap14.htm

According to judicial interpretation, investigation consists generally of the following steps[1435]:

1. Proceeding to the spot;

2. Ascertainment of the facts and circumstances of the cases;[1436]

3. Discovery and arrest of the suspected offender;

4. Collection of evidence relating to the commission of the offence which may consist of:

(a) the examination of various persons (including the accused) and the reduction of the statements into writing, if the officer thinks fit;

(b) the search of places or seizure of things considered necessary for the investigation are to be produced at the trial;[1437] and

5. Formation of the opinion as to whether on the material collected there is a case to place the accused before a Magistrate for trial, and if so taking the necessary steps for the same by the filing of a charge sheet Under Section 173 of Code of Criminal Procedure.[1438]

Compoundable Offences among Cyber Crimes

An offence which can be legally settled for consideration between the party against whom the offence is committed and by whom the offence is committed is said to be compoundable offence Offences punishable with imprisonment of up to three years are compoundable by a competent court. However, repeat offenders cannot have their subsequent offences compounded. Additionally, offences which affect the socio-economic conditions of the country or those committed against a child under 18 years of age or against women cannot be compounded.[1439] Compounding means

[1435] Central Bureau of Investigation (CBI), Chapter 14: General Instructions Regarding Investigation & Enquiries, available at: http://cbi.nic.in/aboutus/manuals/Chapter_14.pdf
[1436] Ibid.
[1437] http://apvc.ap.nic.in/js/vol1/c12t1s2.html
[1438] Ibid.
[1439] 77A. Compounding of Offences.- (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

complainant will compromise with the accused and withdraw his criminal complaint, which is normally not possible with any offence. Sec 324 of Cr.P.C prescribes the procedure to compound the offence. Same procedure shall be followed for cyber offences as well.

Agencies which are investigating cyber crime

With increased use of computers in homes and offices, there has been a proliferation of computer-related crimes. These crimes include: (i) Crimes committed by using computers as a means, including conventional crimes. (ii) Crimes in which computers are targets.

Central Bureau of Investigation

The increased use of networks and the growth of the Internet have added to this complexity. The Internet is the single, richest and most frequently updated information resource on Computer Crimes. With highly systematic and structured searching techniques available, it is easy to go to the specifics one has in mind. CBI Officers are advised to use the Internet as a resources for any new technological challenges. To combat computer-related crimes, the CBI has the following specialized structure[1440]-

- Cyber Crimes Research and Development Unit (CCRDU);
- Cyber Crime Investigation Cell (CCIC);
- Cyber Forensics Laboratory; and
- Network Monitoring Centre.

Cyber Crimes Research and Development Unit (CCRDU)

The CCRDU is charged with the responsibility of keeping track of the developments in this ever-growing area. The CCRDU is primarily involved in the following tasks:

a) Liaison with the State Police Forces and collection of information on cases of Cyber Crime reported to them for investigation and to find out about the follow-up action in each case;

pending for trial and the provisions of section 265 B and 265C of Code of Criminal Procedures, 1973 shall apply

[1440] http://www.cbi.nic.in/

b) Liaison with software experts to identity areas, which require attention of State Police Forces for prevention and detection of such crimes with a view to train them for the task;

c) Collection of information on the latest cases reported in other countries and the innovations employed by Police Forces in those countries to handle such cases;

d) Preparation of a monthly Cyber Crime Digest for the benefit of State Police Forces; and

e) Maintenance of close rapport with the Ministry of IT, Government of India and other organizations/Institutions and Interpol Headquarters,. Lyon for achieving its objective of giving the needed thrust to collection and dissemination of information on Cyber Crimes.

Cyber Crime Investigation Cell (CCIC)

The CCIC, established in September 1999, started functioning from March 2000. It is a part of the Economic Offences Division.[1441] The Cell has all-India jurisdiction and investigates criminal offences under the Information Technology Act, 2000, besides frauds committed with the help of computers, credit card etc. It is also a round-the-clock Nodal Point of contact for Interpol to report Cyber Crimes in India, and also a member of ―Cyber Crime Technology Information Network System‖ of Japan.

The Cyber Forensics Laboratory (CFL)

The Cyber Forensics Laboratory (CFL), established in November 2003, functions under the Director, Central Forensic Science Laboratory. The responsibilities of CFL are:

i. Provide media analysis in support of criminal investigations by CBI and other Law Enforcement Agencies.

ii. Provide on-site assistance for computer search and seizure upon request.

iii. Provide consultation on investigations or activities in which media analysis is probable or occurring.

iv. Provide expert testimony.

[1441] http://cybercrime.planetindia.net/cybercrime_cell.htm

The following principles are followed by the CFL:

i. The purpose of the analysis shall be to use the evidence in the Court.

ii. All legal formalities shall be followed.

iii. The media should have been legally seized and chain of custody maintained.

iv. The analysis shall be on an image of the media and not on the media itself.

v. The laboratory shall have the best imaging tools and software tools for analysis.

The Network Monitoring Tool (NMT)

The purpose of the Network Monitoring Centre is to police the Internet. It has a Network Monitoring Tool (NMT) developed by I.I.T., Kanpur and may use similar and other tools to achieve its purpose after following the required procedure.[1442] When the Investigating Officer is required to carry out search in a place where it is suspected that computer or computer networks or any other electronic memory devices are likely to be found, it is advisable to contact computer forensic scientists of a Forensic Science Laboratory to accompany the search team. In case, it is not possible, information may be collected regarding the type, make, model, operating system, network architecture, type and location of data storage, remote access possibilities etc., which can be passed on to Forensic Experts as that would help making necessary preparation to collect and preserve evidence. It must be remembered that on some occasions, it may not be possible to remove the computer system physically and data may have to be copied at the scene of crime/place of search. The Investigator or expert must carry necessary media, software, and other specialized items as well as special packing materials which can prevent loss of data as data of magnetic media can be destroyed by dust, jerks and electrostatic environment.

Police Special cyber cell

Delhi Police Crime cyber cell

In a bid to speed up investigation in cases related to IT Act which have more than doubled in the last four years, a dedicated cyber cell for the Crime Branch was inaugurated today by Delhi Police Commissioner B S Bassi. The police chief directed

[1442] http://cbi.nic.in/aboutus/manuals/Chapter_18.pdf

his force to make effective use of the existing facilities and further make it a state-of-the-art centre for cyber crime investigations.[1443] The cyber cell will function from Old PS Kotwali building, Daryaganj, New Delhi. "Cyber Crime cases have witnessed a quantum jump over the past few years. These complaints are being received by hand as well as through post or e-mails and are generally related to social networking sites like Facebook, Twitter, Youtube besides fake e-mail IDs, hacking of websites, e-mail accounts, credit card frauds, internet banking, frauds, abusive, defamatory or threatening e-mails.[1444] The evidence in such cases is required to be immediately retrieved and analysed. Since the evidence pertains to e-mails, websites, chat rooms and databases has to be traced on the desktops, laptops as well as mobiles phones, it is imperative that the data is retrieved at the earliest and following the prescribed procedure for its admissibility in courts.[1445] Thus, in order to investigate cyber crime cases and quickly retrieve or analyse important and relevant data, a separate cyber cell has been set up in the Crime Branch which will deal with cases related to cyber crime in Delhi.This cyber cell will work in tandem with the cyber cells of EOW and Special Cell.The cell will start functioning under the guidance of Deputy Commissioner of Police.

Powers of Police Officers in Investigating Cyber Crime

Power to Confiscate, Section 76 IT Act

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.[1446] Section 76 lays down the conditions under which documents or things which contain any information about the cyber crime or were used in committing the crime can be confiscated by police or investigating officer. Some of the things which can be confiscated are hardware which can include any data-processing devices (such as central processing units, memory typewriters, laptop or notebook computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes,[1447] optical storage devices, transistor-like binary devices, and other memory storage devices), peripheral input or output devices (such as keyboards, printers, scanners, plotters,

[1443] www.delhipolice.nic.in
[1444] http://www.business-standard.com/article/news-ians/delhi-police-crime-branch-gets-cyber-cell-115041301103_1.html
[1445] http://www.ndtv.com/delhi.../delhi-police-crime-branch-gets-dedicated-cyber-crime
[1446] The Information Technology (Amended)Act, 2008
[1447] http://forums.bizhat.com/showthread.php/24291-Computer-Crimes-and-the-Act

video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices).[1448]

Power of Police Officer and Other Officers to Enter, Search, etc, Sec 80 of IT Act

This section empowers police with vast powers to search premises and arrest suspected accused. This provision empowers police to arrest by way of preventive action i.e., if police can suspect that a person is going to indulge in a cybercrime before he plunge into action police officer can arrest him. Another power given to police officer is arrest without warrant.[1449]All cybercrimes are recognized as cognizable offences. Sec 41 of Code of Criminal Procedure confers powers to arrest without a warrant in some grave and urgent situations. The rationale behind giving this power to police is to prevent accused from absconding. After arrest a police officer shall produce the arrestee in front of the nearest magistrate within 24 hours. A judge after perusing facts of the case will either send the person to police custody or judicial custody under as per section 164 of Cr.P.C for further investigation and collection of facts. Unless the accused is a dangerous criminal police shall not hand cuff him. Arrest can be courted by word and if he surrenders to police there is no need to handcuff him. Sec 43 of Cr.P.C gives power to go to extent of killing the accused if he is trying to evade arrest. But from the language of the section it is clear that it shall be the last resort. All these powers could be exercised by not only a police officer but according to the Act any officer appointed and authorized by Central or State Government can exercise with a condition that he or she shall handover the person or present him in from of the judicial magistrate without any delay.

Search of place entered by person to be arrested, Section 47 Cr.P.C, 1973:

A Police officer is empowered to search anywhere in India outside his jurisdiction if necessary. In general they take the help of local police. He can make an arrest by breaking the door and windows of such house or place

Power to Search persons, Section 156 Cr.P.C, 1973.

[1448] Ibid.

[1449] http://www.communitylaw.org.nz/community-law-manual/chapter-28-police-powers/police-powers-of-arrest/

Police officer's power to investigate cognizable case.135 Under this section the police is empowered to investigate into a cognizable offence without order of magistrate or without a formal first information report. The statutory right of the police to investigate cannot be controlled or interfered with by the court .Any failure to investigate the offence properly or any irregularity in the investigation does not vitiate the trial unless it results in prejudice to the accused or in miscarriage of justice. On mere suspicion that a person is involved in committing a crime or is potential to commit a crime police can arrest under this provision.

Power to investigate non cognizable offences, Section 155 Cr.P.C, 1973.

This section deals with the substance of the information relating to the commission of cognizable offence lodged in a police station, shall be entered in the station diary136 and the police can immediately go to the scene of offence arrest all suspected accused without a warrant, collect evidence and record statements of witnesses.

Power to issue summons, Section 91 Cr.P.C., 1973

Summon to produce documents. If a police officer has information that a person is in possession of some incriminating material such as floppy drives or pen drives etc, he can send summons to that person and ask him to produce the document or a thing to the police officer for the purposes of investigation..This section deals with the production of only such documents which form the subject of a criminal offence or which can be used as evidence in support of a prosecution. Summon are written orders addressed to a person in whose possession the required document or a thing is available. Summon are generally served in person, and if he or she is not available

Power to require attendance of witnesses, Section 160 Cr.P.C., 1973

As per this provision the Investigating Officer can summon persons who are acquainted with the facts of the case138 or can give some information about the offence could be summoned to come to the police station and give statements. These statements shall be recorded by Police officer and need not be signed by the maker of statement. These statements are called as 161 statements, which can be used during trial.

Power to issue Search Warrant, Section 93 Cr.P.C., 1973

This is a general provision as to search warrants. If a person doesn‘t respond to summons or refuses to receive summons the next coercive method available in criminal procedure is issuing of search warrant. In this process a police officer is entitles to enter any premises and search it and seize documents, which are useful for the investigation. This section will apply not only when an inquiry is pending but also when an inquiry is about to be made.[1450]

Procedure for search, Sec 100 of Cr.P.C, 1973

This relates to search, wherein a police officer can enter the premises and has to prepare a seizure memorandum which contains a list of things seized in the said house. The search process shall be conducted in the presence of two respectable inhabitants of the same locality.[1451] They have to sign the seizure memorandum. The generic consistency one encounters in penal laws permits a broad analysis of how these laws can be adapted to deal with cybercrime. Such an analysis is more problematic when one turns to procedural law, since there is much more variation among nations in this area. Notwithstanding that, it is important at least to note how procedural law may need to be revised to facilitate the investigation and apprehension of cybercriminals. After all, a country can have a comprehensive penal code that reaches every known variety of cybercrime but still be unable to prosecute cybercriminals because of gaps in its procedural law.

Cybercrime is often transnational crime, which raises the issue of jurisdiction to prosecute the offender. Countries must examine their procedural law and, if necessary, amend it so they can legitimately exercise jurisdiction over cybercrimes. Traditionally, jurisdiction has been equated with territory, with the scope of a country's being defined by the limits of its territorial boundaries.[1452] This territorial notion of jurisdiction to prosecute becomes problematic when dealing with cybercriminals. Determining where a cybercrime was ―committed‖ can be difficult, since the perpetrator and the victim can be located in different countries and since the perpetrator may utilize computer systems in several countries in the course of attacking the victim. One approach to this problem is to broaden the territorial notion

[1450] S.V. Joga Rao, Law Of Cyber Crimes & Information TechnologyLaw, Wadhwa & Company Nagpur ,New Delhi,2004 P. 89
[1451] The Code of Criminal Procedure, 1973
[1452] http://conventions.coe.int/treaty/EN/cadreprojets.htm.

of jurisdiction to prosecute so that it allows the nation to prosecute whenever the offender's conduct occurred in whole or in part in the prosecuting nation's territory.

This approach would, for example, give the country jurisdiction to prosecute a cybercriminal (a) when both the victims and the perpetrator were located in the country at the time the crime was committed and the perpetrator utilized computer technology located in that country; (b) when either the victim or the perpetrator was located in that country during the commission of the crime; and (c) when any part of the crime was committed, planned or facilitated in that country. Finally, countries can impose their own penal law on their citizens when the citizens are abroad, which means that a country could prosecute one of its nationals for committing a cybercrime even though the actual commission of the offense was carried out in another country and did without a warrant of have harmful effects on people or property located within the prosecuting jurisdiction.

Bail provisions for Cyber Crime

There are two classes of offences, bailable and non-bailable recognized by Code of Criminal Procedure that is, bailable and non-bailable offences. Bailable offences are petty offences whereas non-bailable offences are serious offences. When an accused is arrested for the alleged commission of a cyber crime he can apply for bail. If the offence is bailable, court grants bail to him under sec 436 of CrPC. If the offence alleged is non-bailable, court grants bail Sec 437 or 439 of CrPC. There is another classification on the basis of power of police to arrest the accused, i.e., cognizable and non cognizable offences, for a cognizable offence police officer can arrest the accused without a warrant and for a non cognizable offence he cannot do so.

Information regarding the fact that whether a particular offence is bailable or not is available in the first schedule of CrPC. It is brought that the offence under Sections 65 and 66 of the Information Technology Act is bailable in view of Section 77B of the Information Technology Act.[1453] However, Section 77B has been inserted under 2008 IT Amendment Act as per which the offence punishable with imprisonment of three

[1453] www.cybercrimelawyer.wordpress.com/category/bail-in-section-66-of-information-technology-act

years and above shall be cognizable and the offence punishable with imprisonment of three years shall be bailable.[1454]

Sec.77B offences with three years imprisonment to be cognizable-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.[1455]

CONCLUSION

The lack of adequate penal laws will prevent the offender's being prosecuted in his own country, will prevent his being extradited to the countries he has victimized and can hamper law enforcement's ability to investigate and apprehend him. One nation's inadequate penal laws can result in the victimization of citizens of other countries, countries which have tried to protect their citizens by adopting laws adequate to prohibit the conduct at issue. But it is not only remote cyber offenders who exploit gaps in penal laws. A cybercriminal can take advantage of such gaps to commit crimes against individuals and or businesses in his own country, knowing he cannot be prosecuted for what he does. The obvious solution to both forms of exploitation is for countries to ensure that their penal and procedural laws are adequate to permit the investigation and prosecution of cybercriminals. Indeed, this is a central feature of two conventions that have been drafted to deal with cybercrime. Legislative responses to cybercrime should be both rigorous and conservative.

[1454] According to Section 2 (a) of CrPC, — bailable offence‖ means an offence which is shown as bailable in the First Schedule, or which is made bailable by any other law for the time being in force: and —non-bailable offence‖ means any other offence

[1455] The information Technology Amended Act, 2008 Talat Fatima, Cyber Crimes, Eastern Book Computer, Lucknow, 2011, p.445