CYBER CRIMES: ROLE OF LAW ENFORCEMENT AGENCIES

Written by ***Ann Clara Tomy***

2nd Year BBA LLB Student, School of Law Christ (Deemed to be) University

INTRODUCTION

India, today, is the seventh largest country with a total area of 3.287 million square kilometers and the second most populous country with a population of 1,21,05,69,573.[1]Over the past few decades, the nation has grown considerably in size, population and infrastructure and this has simultaneously led to numerous challenges and difficulties in the realm of governance. The functioning and working of the country is guided by the principles enshrined in the Constitution which was adopted on 26th January 1950. With respect to governance in specific, Article 248 of the constitution deals with the apportionment of law making power between the centre and the state legislature by providing a separate list of subjects that can be governed by the Centre and State.[2] Police, Public order, courts, prisons, reformatories, borstal and other allied institutions which play prominent role in executing the law have been placed in the State list. Among these subjects, "Police" is a highly important and sensitive institution and the superintendence over the police force is exercised by the State Government.[3] They play a pivotal role in law enforcement and maintenance of law and order in the country. In recent times one of the most notable reasons of disturbed law and order has been cyber violence. The rapid growth in technology coupled with hike in usage of online means entwined with malicious intent of deploying such advancement for financial personal gains has led to a sharp increase in the number of cybercrimes that can take place in the online environment. Hence cyber safety is an arena of importance for the law enforcement agencies today.

[1]Census of India 2011, Office of registrar general and census commissioner(June 20,2018,9:00am),http://www.censusindia.gov.in/2011census/PCA/PCA_Highlights/pca_highlights_file/India/Chapter-1.pdf
[2]Article 248,Constitution of India
[3]Section3, The Police Act 1861

THE POLICE FORCE AND ITS STRUCTURE

The policing mechanism in our country is mainly of two types: firstly, the dual control system of policing[4] and secondly, the Commissionerate system of policing. Under the dual system of policing, the entire force is placed under the District Superintendent of Police but however was subject to the general control and direction of District Magistrate. The dual system posed many challenges to the smooth governance of the force due to lack of clarity in demarcation of powers vested with the Superintendent and Magistrate, this led to constant conflicts and chaos especially in Metropolitan cities due to its population density and unique law and order situations and hence the Commissionerate system was introduced. Under this system the responsibility for policing a city is vested with the Commissioner of Police of the city.

With respect to designation and power, the police force has a hierarchical setup with the Police constable and Director General of Police at the two extremes of the organisation. The total civil police force in the country is 19,89,295 and the ratio of number of police personnel per lakh of population is 192.87. A detailed breakup of the force strength shows that the total number of level 1 officers which include DGP, ADGP, IGP, DIG, SP, DySP is 19,380 (0.7%) while the total number of level 2 officers which include CI,SI and ASI is 3,52,352(14.3%) and the total number of level 3 officers which comprises the constabulary is 20,92,752(85%)[5]. The major part of the police force consists level 3 officers, they play an enormous role in ground level implementation of laws and are required to directly deal with the public and their grievances on a frequent basis.

The recruitment to the state police is usually done at three levels- Constable, Sub Inspector/Asst. Sub Inspector and Deputy Superintendent of Police. There is direct recruitment to the Indian Police Service (IPS) at the level of Assistant Superintendent of Police. The Constables are recruited directly since it is at the lowest level in the police structure hierarchy and the other posts may either be filled by direct recruitment or by promotion. The selection process to the post of a constable involve physical examination, efficiency test, written examination, medical examination and interview which is conducted by a board presided by the Superintendent of Police. For the post of a Sub Inspector, the selection process is governed

[4]Section4, The Police Act 1861
[5]Data on Police Organisations, Bureau of Police Research and Development(June 22,2018,4:10pm), http://bprd.nic.in/WriteReadData/userfiles/file/databook2017.pdf

by the State Public Service commission while the recruitment to the Indian Police Service is done by the Union Public Service Commission through a rigorous selection process which includes a national level aptitude test followed by interview and standardised training.

The inception of law dealing with law enforcement agencies in India dates back to the year 1861, when the first Police Act was enacted. This colonial legislation was continued even after independence and thereafter no central legislation was formulated for the governance of the police force in the country. However it cannot be implied that there have been no efforts to revamp the police structure and to bring in reforms in the force. Several expert bodies have worked relentlessly time to time assessing the functioning of the police force and suggesting ways to improvement. An innovation in this regard was the initiation of the National Police Commission which was appointed by the Government of India in 1977 with wide terms of reference covering various aspects relating to police setup. The commission has submitted eight reports between 1971 and 1981 with various progressive recommendations. Further the Riebero commission report[6], Padmanabhaiah committee report[7], Malimath committee report[8] elaborated on the need for improved police strength, improved police accountability as well as a revised Police Act. A significant development in the area of police governance took place after the Supreme Court decision in the Public Interest Litigation Prakash Singh v Union of India[9] case in which the court issued directions to enact State legislations that will be able to effectively govern the activities of the police force and also increase their commitment and accountability. In advancement to these developments a Police Act drafting Commission also known as Soli Sorabjee Committee was constituted in the year 2005 which drafted a Model Police Act in the year 2006[10], after nearly ten years in 2015, again a Police Act drafting Committee was set up and a Model Police Act was proposed which is in public domain for comments. Apart from these committees and their reports, there are governmental organisations set up for the systematic development of the police force, research on the efficiency of policing and to constantly recommend needed reforms to the government. In

[6]Ribeiro committee's recommendations, Commonwealth Human Rights Initiative(June 19,2018,10 am), https://humanrightsinitiative.org/old/publications/police/recommendations_ribeiro.pdf
[7]Padmanabhaiah committee's recommendations, Commonwealth Human Rights Initiative(June 19,2018, 12 am), http://humanrightsinitiative.org/programs/aj/police/india/initiatives/analysis_padmanabhaiah.pdf
[8]Malimath committee, Ministry of Home Affairs India (June 22,2018,1:30pm), https://mha.gov.in/sites/default/files/criminal_justice_system_2.pdf
[9]Writ Petition (civil) 310 of 1996
[10]Model Police Act 2006, Commonwealth Human Rights Initiative(June 19,2018,5pm), http://humanrightsinitiative.org/old/programs/aj/police/india/acts/model_police_act_2006.pdf

accordance with the recommendations of the 1977 National Police Commission Report, The Ministry of Home Affairs in the year 1985 set up a task force to study the feasibility of setting up an institution to centrally track the crimes in the country and to ensure better crime detection, prevention and policing mechanism throughout the country. As a result of this endeavour the National Crimes Bureau was formed in 1986[11]. Bureau of Police research and development was established under the Ministry of Home Affairs giving a new orientation to the Police Research and Advisory Council (1966) with the primary objective of modernization of police.[12]

CYBER CRIMES AFFECTING COMMON MAN

"Cyber Security is crucial, Govt. Websites also get hacked and misused due to which public is often misled with information"-Justice Lokar[13]

The police today are faced with not just conventional crimes, with evolution in technology and advancement in science; they are challenged with unique cases every now and then. The most prominent these days are cybercrimes. Cyber violence has evolved as a phenomenon and has caused devastating effects in the lives of common man. It leads to social, political, economic, physical as well as psychological adverse results on the victims.

There are certain reasons why cybercrimes are unique from other crimes. Firstly, the offender is given the golden opportunity of maintaining anonymity. It is hard in most case to trace the attacker. Secondly, the ease of learning how to use the internet coupled with access to millions of users make the process of online abuse fairly simple. Thirdly, the permanency of digital information. As the saying goes "The internet never forgets anything", this makes users prone to cyber-attacks and cyber threats that are formulated with the help of personal sensitive

[11]Message from Director's desk, National Crime Records Bureau (June 25,2018,7 pm), http://ncrb.gov.in/
[12]Evolution of BPRD, Bureau of Police Research and Development(June 22,2018,8 am), http://bprd.nic.in/content/11_1_EvolutionofBPRD.aspx
[13] International conference on cyber law, cyber crimes and cyber security2016, International conference on cyber law, cyber crimes and cyber security(June 23,2018,9 am), http://cyberlawcybercrime.com/previous-iccc/iccc-2016

information posted online. There are mainly two types of cybercrimes: Crimes in which computer acts as means and Crimes in which computer acts as targets.[14]

The cyber threats that the citizens of today face are plenty which include Work from Home scam, Online Banking scam, Cyber stalking, Romance Scammers, Cyber harassment. Work from home is an attractive concept as there plenty of advertisements today that offer high remuneration for simple works. The application for such advertised jobs will include giving several vital personal information and details. Further these ads entice people to refer the same to others by providing incentives. However there have been several cases reported that the personal information acquired through these applications have been misused and have in worst scenarios have been used to commit crimes. Bank fraud cases have become everyday phenomena and have been increasing consistently over the past few years. In 2016, 3156 cases and 4147 cases were registered in the September and December quarters respectively and in 2017 over 25,800 cases involving about 179 crore were reported.[15]Crime Statistics report states that the number of cybercrimes has been steadily increasing, the number being 9,622 in 2014, 11,592 in 2015 and 12,317 in 2016. There is a huge pendency of cybercrime cases in the country, according to latest available data a total of 10164 trial cases are pending which leads to a pendency of 92.3%.[16]

The sole legislation enacted to cope up with the rising level of cybercrimes is the Information Technology Act 2000. Section 43 of the Act elaborates the penalty and compensation for unauthorised access to one's computer, computer system or computer network. Section 43A provides for compensation for failure to protect data. It makes liable anybody corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, if it is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any

[14]Crime Statistics 2016,National Crime Records Bureau (June 18,2018,1:45pm),http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf
[15]Over 25800 online banking fraud cases reported in 2017 says government, The Hindu, December 29, 2017,http://www.thehindu.com/business/Economy/over-25800-online-banking-fraud-cases-reported-in-2017-says-government/article22327229.ece
[16]Crime Statistics 2016,National Crime Records Bureau (June 18,2018,1:45pm),http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf

person[17].Further Section 66D of the Act provides for punishment for cheating by personating using computer resource. The IT Act also provides for a mechanism to deal with cybercrimes. Chapter IX and Chapter X deals with grievance redressal setup formulated. It provides for the appointment of an adjudicating officer who shall be an officer appointed by the Central Government not below the rank of a Director to the Government of India or an equivalent officer of State Government. The adjudicating officer has jurisdiction to adjudicate matters in which claim for injury or damage does not exceed 5 crores. The adjudicating officers are instructed to handle cases faster and to avoid long pendency of cases. Cases are generally expected to be disposed off in 6 to 9 months. The Act also provides for an Appellate Tribunal which is the Telecom Disputes and Settlement and Appellate Tribunal established under Section 14 of the Telecom Regulatory Authority of India Act 1997.

POLICE INSTITUTIONS THAT DEAL WITH CYBER CRIMES

Enactment of laws is definitely a vital part of dealing with a certain set of problems in the society however enactment without enforcement will yield no positive effects. This is where there comes the need to analyse the pivotal role played by the law enforcement agencies or in simple terms the police force of the Nation. The laws have also authorised the police to perform vital tasks predominantly important for handling cybercrimes. Information Technology Act 2000 for instance empowers police to enter any public place to 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 the Act[18]. Further any information or matter which is rendered or made available in an electronic form and is accessible so as to be usable for a subsequent reference is legally recognised as evidence,[19] this gives arms to the power of police to conduct searches and collect evidences which are electronic in nature. The general scheme of investigating a cybercrimes include: Formulating an Advance Plan, Depriving further access to the attacked computer resource, Precautionary steps to ensure

[17]Section 43A, IT Act 2000
[18]Section 80, IT Act 2000
[19]Section 4, IT Act 2000

investigation goes on smoothly, Seeking help of a forensic expert in case of unavailability of specialist seizure of everything and protecting the collected data and transporting it safely.

The structure of cyber policing in the country is governed by the Central Bureau of Investigation (CBI). The primary Institutions that deal with cybercrimes are Cyber Crime Research and Development Unit, Cyber Crime Investigation Cells, Cyber forensic Labs, Network Monitoring Centres. These central organisations govern the cybercrime detection and investigation across the country. They ensure cooperation with the State Police Force and also are responsible for finding out and following up actions taken by Inspecting Officers (IO) in important cases. In addition forensic labs have been setup in every district to facilitate the control of cybercrimes. A key innovation of the central body CBI is the Cyber and Hi Tech Crime Investigation and Training Centre (CHCIT). It functions at the CBI academy. The centre has provided technical and forensic assistance during investigation of high profile cases.[20]

CONCLUSION AND SUGGESTIONS

As evident from the facts and figures mentioned in preceding paragraphs, the high level of pending cases, low rate of conviction have led to cyber security being an arena that requires immediate attention. The majority of the cases are those that involve common man as victims compared to those that affect big corporate. Given this proportion of higher number of cyber cases affecting middle class, a mechanism must be devised so as to ensure that such small scale frauds are efficiently detected and controlled. The present measures taken by the government and government established organisations mainly place importance in high profile cases and hence there is dire lag in taking notice of other cases that are unlikely to draw much media attention. This is where the role of local police comes into picture. Being at the lowest level of the police hierarchy the constabulary play a major role in interacting with the public, addressing their grievances, aiding preliminary investigation and ensuring awareness among the public. The local police need to be equipped to attend to cyber complaints and effectively act on it. They require the skills to be able to seize valuable evidence from the crime resource which is crucial for handling cybercrimes. The most challenging part of a cybercrime investigation is

[20]Cyber and Hi Tech Crime Investigation and Training Centre (CHCIT), CBI Academy(June 26,2018,12 pm), http://www.cbiacademy.gov.in/chcit.php

evidence collection, when the cases reach the court without efficient preliminary investigation evidence it leads to acquittal of the accused. The cyber investigation cells established specifically to handle cybercrimes are in most states empowered to handle only cases which are above a certain value. For instance, in Bangalore, pursuant to a standing order by the DGP only bank fraud cases of 5 lakh and above and cheating cases of 50 lakh and above could be handled by the cyber cell[21]. This shows that the innumerable number of cases involving a subject matter of value lower that the prescribed limits need to be reported in local police stations which directly leads to requirement of trained personnel in local police stations.

Therefore the lower rank officials need to be equipped with adequate skills and need to be given considerable power to deal with such situations. However in the present governance structure the constabulary is not given due importance and hence the quality of training and attention given to enhance their skills is very minimal. Basic skills required to handle small scale cybercrimes must be provided to the constables especially those recruited to urban police stations which deal with a considerable number of cyber frauds. Such focused training and capability enhancement can go a long way in controlling cyber threats as most cases are not successful due to confusion of the police regarding what has to be done when such types of cases are reported.

Apart from training the other aspect that requires attention is providing the officials with adequate power. Section 80 of the IT Act states that no officer below the rank of Deputy Superintendent of Police (DySP) can enter any public place and search without warrant. This limits the power of the lower officials and also brings delay in the process as it involves a higher authority's intervention. However such powers can be given to the lower officials only when they are efficient enough to handle cases that involve cyber complexity.

For the aforesaid to happen there is severe requirement of resources that needs to be allocated to the police in order to upscale the training sessions and also build cohesive institutions to handle the rising diversity of crimes which is a of today primarily cybercrimes. The budget analysis proves that, the share allocated to building police infrastructure is underutilized. According to latest available data, in 2015-16 out of the total grant of 9,203 crore made

[21]Bengaluru police's first cybercrime station maybe of little help, Times of India(June25, 2018,8:40 am), https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-polices-first-cybercrime-station-may-be-of-little-help/articleshow/56846307.cms

available to the states for modernisation only 1330 crore i.e. 14% was utilised.[22]Hence the present state of affairs evidences the low priority given to modernising and equipping the police force. Active political will and clearly planned agenda is urgently required to adequately train the officers especially those at the lower level.

Further it is required bring in reformations to recruitment of constabulary. The recruitment should involve a separate selection process for candidates interested in being cyber experts and handling cyber resources, the educational qualification for such posts must be hiked. Such demarcation will incentivize youngsters to join the police force and will streamline the process of imparting extensive coaching on handling cybercrimes. Apart from detecting and handling cybercrimes, local police also play a key role in spreading awareness about the rising menace of cybercrimes. Being in a position to constantly interact with the victims and the general public, the lower officials are most favourably placed to undertake the responsibility of alerting citizens about cyber safety. Such efforts can considerably decrease the number of cyber fraud incidents that take place due to the carelessness and ignorance of the user. Changes in the abovementioned regard can enhance cybercrime tackling skills of the police force and to a great extent ensure a cyber-safe environment to the common man.

[22]Budget 2018:Police modernisation, infrastructure, forensics, Financial Express (June 19,2018,10am), https://www.financialexpress.com/budget/budget-2018-for-police-modernisation-infrastructure-forensics-case-for-increase-in-police-budget-and-why-it-needs-to-be-monitored/1037419/