WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Investigation and Adjudication of Cybercrimes in India

Gokul Sangeetha.R

B.Com.L.L.B.(Hons), The Tamil Nadu Dr. Ambedkar Law University, School of Excellence in Law, Chennai.
DOI: https://doi.org/10.55248/gengpi.234.4.38093

ABSTRACT

Now a days the basic need of humans are food, water, shelter and internet. The internet in our daily life has become one of the member of our family. It occupies our spaces in much larger. Although internet is a medium of learning, entertainment, technology, knowledge, art, science, etc., it has a both advantage and disadvantage over it. The cyber space which is a digital space in which all the technology based ideas were created, designed and which leads to male use of people. The people in every country were relied on the internet which affects the minds of people and it causes the offences in cyberspace. The cybercrimes, offences, attacks which were considered as an inappropriate cause to the cyber world. To avoid these issues the Information Technology Act,2000 was created and in that the process for cybercrime rules, regulation, procedures, investigation, adjudication, penalization, compensation, etc., were stated.

KEYWORDS: Internet, Cybercrime, Investigation, Adjudication, Punishment, Compensation, IT Act,2000.

INTRODUCTION

In India, the Information and Technology Act, 2000 was the main area for cyber laws. Internet law which means cyber law which mainly focuses on cybercrimes, cyber stalking, cyber pirates, cyberspace censors, cyber spoofing, cyber phishing, cyber hacking, cyber terrorism, cybersquatting, etc. The IT Act was enforced for the cybercrimes & Ecommerce which took place in India. In recent days the emergent of cyber space has increases rapidly which ultimately leads to cyber offences. This article deals with investigation and adjudication of cybercrimes in India.

CYBERCRIME AND INFORMATION TECNOLOGY ACT, 2000

The usage of internet when increases to its extent limit, there causes cybercrimes. The cyber laws mainly focuses on the crimes which related to internet access. Now a days the access of internet through online shopping, ebanking, ehealth, online classes, social media & etc., were become wider than its establishments so by using this we were blindfolded & which leads to cyber offences. In India cybercrimes activities were regulated by the Information Technology Act, 2000. The Act which includes the procedures, detention, investigation, adjudications, punishments, orders, inquiries, rules and regulations, etc .

The cyber offences were also stated under the Indian Penal Code (IPC) &its includes crimes like theft, cheating by impersonation, mischief by damaging computer systems, and publishing obscene material in electronic form & states about the punishment of those who are found guilty of cybercrime. Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet.[1]

This Act, passed with the objective of promoting a secure electronic environment deals with issues subsidiary to this secure electronic transactions and information technology offences.[2]

ESSENTIAL INGREDIENTS OF CYBERCRIME

It is a general principle of criminal law that a person may not be convicted of a crime unless the prosecution has proved beyond reasonable doubt that:

- He has caused a certain event, or responsibility is to be attributed to him for the existence of a certain state of affairs, which is forbidden by criminal law; and
- He had a defined state of mind in relation to the causing of the event or the existence of the state of affairs.[3]

[1] See<https://www.britannica.com/topic/cybercrime>

[2] See, the Nandhan Kamath's Law Relating to Computers Internet & E-commerce, published by Universal Law Pubishing, fifth edition, p.229

CYBERCRIME INVESTIGATION IN INDIA

To know cybercrime investigation, we have certain special equipmental knowledge and scientific tools are required without this the investigation woudn't get start. The Indian legal system has structured many procedures, rules, regulations which are enacted it in a statute. The technological advancements and developments have inverted in the digital India for its progression. Cyber-crimes usually transgress geographical hurdles. Cyber-crime is a fast-growing meadow of crimes. The Cyber criminals are exploiting the speed barriers and anonymity of the internet for the commission of different types of criminal activities. No border, virtual or physical, can cause serious harm and rise real threat to worldwide victims other than Cyber-crimes. In order to deal with the issue of Cyber-crimes, the Criminal Investigation Department (CID's) of various cities established, Cyber Crime Cells (CCC) in various parts of the country. The IT Act, 2000 made it clear.[4]

The cybercrime investigation is the process of investigating, analyzing and recovering critical forensic digital data from the networks involved within the attack this might be the web and/or an area network—in order to spot the authors of the digital crime and their true intentions.

CYBERCRIME INVESTIGATORS

The investigators must be experts in computing, understanding not only software, file systems and operating systems, but also how networks and hardware work. They need to be knowledgeable enough to work out how the interactions between these components occur, to urge a full picture of what happened, why it happened, when it happened, who performed the cybercrime itself, and the way victims can protect themselves within the future against these sorts of cyber threats.[5] Section 78 of the Act[6] power to investigate offences by police officer which states that "Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of [Inspector] shall investigate any offence under this Act."[7] Section 80 of the same act sates that the police officer which was mentioned under section 78 or any other officers in which the state and central government has authorized power to search at any public place, seize, inquire and even can also arrest the suspected personwho commits the offence.

CYBERCRIME INVESTIGATION METHODS :

While methods may vary depending on the type of cybercrime/cyberattacks were investigated, as well as who is conducting the investigation, most of the digital/ or cybercrimes/attacks are subjected to these common methods used during the investigation process of cybercrime attacks.[8]

COMPLAINT

The cybercrime complaint can be registered under the cybercrime cells. The complaint may be given through online and offline and the complaint can be registered with the convenience of the victim under any cybercrime cells which was established in India. In some case if the victim does not file a complaint under cybercrime cells the he/she can lodge the FIR in the police station under section 154 of Cr.P.C. If the police officers refuses to accept it then the victim can raise a complaint o Judicial Magistrate of the victim's district.

COLLECTING INFORMATION

The investigator may collect the information regarding the cybercrime/cyber attack from the victim, the public and as well as collect the facts, evidence, potential suspects, human planned offence done by any particular or group of persons etc., regarding the offence.

TRACKING

After collecting information, the investigator's next step is oftenly performed during the information-gathering process, depending on how much information and facts is already in gathered. In order to identify the criminals behind the cyberattack, both private and public security agencies often work with Internet Service Providers (ISPs) and networking companies to get critical log information about their connections and networks, as well as historical services, websites and protocols used during the time they were connected. This is often the slowest phase, as it requires legal permission from the prosecutors and a court order to access the needed data.[9]

---

[3]See supra p.210

[4] See International journal of legal developments and allied issues Volume 7 Issue 2 – ISSN 2454-1273 March 2021 https://thelawbrigade.com/

[5]See https://info-savvy.com/cyber-crime-investigation-tools-and-techniques/

[6] The section 78 provided under the Information Technology Act, 2000.

[7]The Information Technology Act, 2000

[8]https://forensicexpertinvestigation.com/cyber-crime-investigation/

[9]https://forensicexpertinvestigation.com/cyber-crime-investigation/

FORENSICS

When the investigator collects all information, data, facts, evidence, etc., then he sends it to the forensic department. This process involves analyzing network connection raw data, hard drives, file systems, caching devices, RAM memory and other potential evidences. Once the forensic work starts, the involved investigator will follow up on all the involved trails looking for fingerprints in system files, network and service logs, emails, web-browsing history, etc.[10]

IDENTIFYING

After the report which was officially from the forensics department, then the investigator has identify the suspected person or the person who commits the cybercrime/cyberattack and the they take necessary action against the offender through the proceeding of Cr.P.C.

NATIONAL CYBER SECURITY COORDINATION CENTRE (NCSC)

NCSC is an agency under cybercrime in which it coordinates with different agencies at national level for to secure the cyber related matters.

CYBERCRIME CELL

The cybercrime cell is the main part of cyberspace, in which it handles the investigations proceedings. With establishment of cyber cells in the cosmopolitian cities in India, there is also a need to build a better technology and investigation infrastructure with highly skilled technical staffs at the other hand.[11]

CBI's SPECIAL UNITS[12]

To fight against the cybercrime the CBI has established the special units:

- Cybercrime Research and Development Unit
- Cybercrime Investigation Cell
- Cyber Forensic Laboratory
- Network Monitoring Centre

EXTENDED MODEL OF CYBERCRIME INVESTIGATIONS[13]

- **Awareness** - Recognition that an investigation is needed
- **Authorisation** - For example, through the issuing of a warrant
- **Planning** - Using information collected by the investigator
- **Notification** - Informing the subject and other interested parties that an
- investigation is taking place
- **Search for and identify evidence** - For example locating the PC used by a suspect
- **Collection of evidence** - Potential evidence is taken possession of
- **Transport of evidence** - Transported to an appropriate location
- **Storage of evidence** - Storage methods should reduce the risk of cross
- contamination
- **Examination of evidence** - The use of specialist techniques e.g. recovery

[10] https://forensicexpertinvestigation.com/cyber-crime-investigation/
[11] https://finology.in/recent-updates/how-cybercrime-cell-works
[12] https://finology.in/recent-updates/how-cybercrime-cell-works
[13] Referred from https://epgp.inflibnet.ac.in/ epgpdata/uploads/epgp_content/S001608/P001742/M027908/ET/1521181215E-Text-CyberPolicing.pdf

- of deleted data
- **Hypothesis** - A tested formulation of what may of occurred
- **Presentation of hypothesis** - For example to a jury
- **Proof/defence of hypothesis** - Contrary hypotheses will also be
- considered
- **Dissemination of information** - The information may influence investigations in the future.

ADJUDICATION OF CYBERCRIMES

The Information Technology Act, 2000 establishes quasi-judicial bodies, such as adjudicating officials, to resolve disputes (offences of a civil nature as well as criminal offences). The adjudicating officer has the jurisdiction to award compensation as a civil remedy as well as impose fines for violating the Act, giving them civil and criminal court-like powers. The Cyber Appellate Tribunal is the first level of appeal, with a Chairperson and any additional members appointed by the Central Government. A second appeal may be lodged with a High Court having jurisdiction within 60 days after the Cyber Appellate Tribunal's ruling has been communicated.[14]

ADJUDICATION OFFICER

Under section 4 of the Act[15] states that, the Central Government in its official notification appoints an officer called adjudicating officer in which it gives the power to make decision. Penalties for the contravention of the provisions of the Act or rules and regulations made there under are adjudicated by adjudicating authority.[16] The appeals from the cases were heard by the Presiding Officer of the Cyber Regulations Appellate Tribunal that was constituted under section 48 of this Act.

COMPENSATION MADE THROUGH ADJUDICATION

Section 43 of the IT Act mentioned that if any person or group of persons causing damage to the computer, computer system, etc., be punished under this provision. The compensation upto one crore of rupees in cases involving:[17]

- Unauthorised access of a computer,
- Unauthorised copying, extracting and downloading of data,
- Introduction of viruses, worms, trojans, etc.
- Damaging or disrupting a computer or network,
- Denying access to a computer,
- Commiting financial irregularites by manipulating computer,
- Facilitating illegal access to computer.[18]

CONCLUSION

Thus the emergent of cyber space in the world has created a special place in the digital technology which will increases the advancement on internet technology and the progression of the society. On one side of cyberspace which leads to the improvements but on other side it creates an open space for cybercrimes, cyber offence, cyber attacks which ultimately causes more offences through the cyberspace which leads to misrepresentation, terrorism, etc. In order to control these offence the Information Technology Act 2000 has the investigation proceeding and the adjudication system in which the

[14] https://blog.ipleaders.in/dispute-resolution-mechanism-of-cyber-laws-in-india/?amp=1

[15] The Information Technology Act 2000.

[16] This is similar to the pattern of Adjudication Officers functioning under the Securities Exchange Board of India Act,1992. However, for the purpose of the I Act 2000, the Adjudicating Officer must posses such experience in the field of information and technology and legal or judicial experience. See Nandhan Kamath's Law Relating to Computers Internet & E-commerce,p229

[17] https://www.asianlaws.org/blog/adjudicating-officers-for-cyber-crimes-appointed-in-india/

matter related to cybercrime were investigated & adjudicated and out of that the offender will be penalized and the victim will be compensated. To decrease the offensive activity the legislature should make a strict construction on the penalized provision of the Act.

REFERENCE

The Information Technology Act,2000.

Nandan Kamath's LawRelaing Computers Internet & E-commerce, Universal law publishing, forwarded by N.R.Madhava Menon – fifth edition.

https://blog.ipleaders.in/dispute-resolution-mechanism-of-cyber-laws-in-india/?amp=1

https://finology.in/recent-updates/how-cybercrime-cell-works

https://forensicexpertinvestigation.com/cyber-crime-investigation/

International journal of legal developments and alliedissuesVolume 7 Issue 2 – ISSN 2454-1273 March 2021 https://thelawbrigade.com/

https://info-savvy.com/cyber-crime-investigation-tools-and-techniques/