INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 3)

Available online at: www.ijariit.com

Cybercrime analysis using criminal information management system: An e-governance measure by ministry of home affairs

Ashish Karan

ashishkaran21@gmail.com

Malaviya National Institute of Technology,

Jaipur, Rajasthan

ABSTRACT

E-Governance is the use of Information and Communication Technology (ICT) to improve the relation between the Government and its citizens. Maintaining effective law and order is one of the primary jobs of the government. Due to limited resources it's very important that the decision makers are provided with reliable data on crime so that resource prioritization can be done effectively. The Ministry of Home Affairs merged the Directorate of Coordination Police Computers (MHA), Inter-State Criminals Data set up of the Central Bureau of Investigation, Crime Statistics set up of the Bureau of Police Research and Development and Central Finger Print Bureau, Calcutta of the Central Bureau of Investigation with the National Crime Records Bureau (NCRB) to streamline the affairs of the E-Governance – Criminal/ Crime Information Management System. The paper endeavors to analyze the trend of Cyber Crime using data from NCRB and correlate it with the offenses in the IT Act.

Keywords: *Cyber Crime, E-Governance, IT Act 2000. Cyber Offence.*

1. INFORMATION TECHNOLOGY LAW IN INDIA

In India, cyber laws are contained in the Information Technology Act, 2000 which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate the filing of electronic records with the Government.

The following Act, Rules and Regulations are covered under cyber laws:

a. Information Technology Act, 2000.
b. Information Technology (Certifying Authorities) Rules, 2000.
c. Information Technology (Security Procedure) Rules, 2004.
d. Information Technology (Certifying Authority) Regulations, 20013.
e. Information Technology (Security Procedure) Rules, 2004.
f. Information Technology (Certifying Authority) Regulations, 2001

The IT Act of 2000 was developed to promote the IT industry, regulate e-commerce, facilitate e-governance and prevent cybercrime. The Act also sought to foster security practices within India that would serve the country in a global context. The Amendment was created to address issues that the original bill failed to cover and to accommodate further development of IT and related security concerns since the original law was passed. The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91,92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008]. Rules notified under the Information Technology Act, 2000

a) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

b) The Information Technology (Electronic Service Delivery) Rules, 2011.

c) The Information Technology (Intermediaries guidelines) Rules, 2011.

d) The Information Technology (Guidelines for Cyber Cafe) Rules, 2011.

e) The Cyber Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Chairperson and Members) Rules, 2009.

f) The Cyber Appellate Tribunal (Procedure for investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009.

g) The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public), 2009.

h) The Information Technology (Procedure and Safeguards for an interception, monitoring, and decryption of information) Rules, 2009.

i) The Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009.

j) The Information Technology (Use of electronic records and digital signatures) Rules, 2004.

k) The Information Technology (Security Procedure) Rules, 2004.

l) The Information Technology (Other Standards) Rules, 2003.

m) The Information Technology (Certifying Authority) Regulations, 2001.

n) Information Technology (Certifying Authorities) Rules, 2000.

2. PENALTIES AND OFFENCES UNDER IT LEGISLATION. THE FOLLOWING ARE THE VARIOUS OFFENCES UNDER THE IT ACT 2000

Section	Offense	Punishment
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs
Sec.43	Damage to computer, computer system, etc.	Compensation not exceeding one crore rupees to the person so affected
Sec.43	Body corporate failure to protect data	Compensation not exceeding five crore rupees to the person so affected
Sec.44(a) failure	Failure to furnish the document, return or report to the Controller or the Certifying Authority	Penalty not exceeding one lakh and fifty thousand rupees for each such failure
Sec.44(b)	Failure to file any return or furnish any information, books or other documents within the time specified	Sec.44(b) Failure to file any return or furnish any information, books or other documents within the time specified Penalty not exceeding five thousand rupees for every day during which such failure continues
Sec.44(c)	Failure to maintain books of account or records	Penalty not exceeding ten thousand rupees for every day during which the failure continues
Sec.45	Where no penalty has been separately	Compensation not exceeding

	provided	twenty-five thousand rupees to the a person affected by such contravention or a penalty not exceeding twenty-five thousand rupees
Sec.65	Tampering with Computer source documents	Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both
Sec.66	Hacking with Computer systems, Data alteration etc.	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both
Sec.66A	Sending offensive messages through communication service etc.	Imprisonment for a term which may extend to three years and with fine
Sec.66B	Retains any stolen computer resource or communication device	Imprisonment for a term which may extend to three years or with fine which may extend to rupees one lakh or with both
Sec.66C	Fraudulent use of electronic signature	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh
Sec.66D	Cheats by personating by using computer resource	Imprisonment for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees
Sec.66E	Publishing obscene images	Imprisonment which may extend to three years or with a fine not exceeding two lakh rupees, or with both
Sec.66F	Cyber terrorism	Imprisonment which may extend to imprisonment for life
Sec.67	Publishes or transmits unwanted material	Imprisonment for a term which may extend to three years and with fine which may extend to five lakh rupees & 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
Sec.67A	Publishes or transmits sexually explicit	Imprisonment for a term which may extend to five years and with fine 57 material which may extend to ten lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees
Sec.67B	Abusing children online	Imprisonment for a term which may

		extend to five years and with a fine which may extend to ten lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees
Sec.67C	Preservation of information by intermediary	Imprisonment for a term which may extend to three years and shall also be liable to fine
Sec.70	Un-authorized access to protected system	Imprisonment for a term which may extend to ten years and shall also be liable to fine
Sec.71	Misrepresentation to the Controller or the Certifying Authority for obtaining license or Electronic Signature Certificate	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.
Sec.72	Breach of Confidentiality and Privacy	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both
Sec.72A	Disclosure of information in breach of contract	Imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both
Sec.73 & 74	Publishing false digital signature certificates	Imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both

3. OFFENCES UNDER OTHER LEGISLATIONS

OFFENCE	LAW
Sending threatening messages by email	Sec.503 IPC (Indian Penal Code)
Sending defamatory messages by email	Sec 499 IPC
Forgery of electronic records	Sec.463 IPC
Bogus websites, cyber frauds	Sec.420 IPC
Email spoofing	Sec.463 IPC
E-Mail Abuse	Sec.500 IPC
Online sale of Drugs	Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985
Online sale of Arms	Arms Act, 1959

4. NATIONAL CRIME RECORDS BUREAU (NCRB)

The NCRB was established in 1986 to function as a clearing house of information on crime and criminals including those operating at National and International levels so as to assist the investigators, and others in linking crimes to their perpetrators.

NCRB developed Crime Criminal Information System (CCIS) in the year 1995, Common Integrated Police Application (CIPA) in

2004, and Crime and Criminal Tracking Network & System (CCTNS) in 2009. The CCTNS connects approximately 15000 police stations and 6000 higher offices in the country. National Digital Police Portal was launched on 21/08/2017, and it allows a search for a criminal/suspect on a national data base apart from providing various services to citizens like filing of complaints online and seeking antecedent verification of tenants, domestic help, drivers etc. (https://digitalpolice.gov.in/). NCRB also compiles and publishes National Crime Statistics i.e. Crime in India, Accidental Deaths & Suicides and Prison Statistics. These publications serve as principal reference points by policy makers, police, criminologists, researchers and media both in India and abroad. The latest Crime in India Statistics 2016 has recently been published by this Bureau and was released by the Hon'ble Union Home Minister on 30.11.2017. Following are the objectives of the NCRB as per government notification.

A. To function as a clearing house of information on crime and criminals including those operating at National and International levels so as to assists the investigators, and others in linking crimes to their perpetrators.

B. To store, coordinate and disseminate information on inter-state and international criminals from and to respective States, national investigating agencies, courts, and prosecutors in India without having to refer to the Police Station records.

C. To collect and process crime statistics at the National level.

D. To receive from and supply data to penal and correctional agencies for their tasks of rehabilitation of criminals, their remand, parole, premature release etc.

E. To coordinate, guide and assist the functioning of the State Crime Records Bureaux

F. To provide training facilities to personnel of the Crime Records bureaux, and

G. To evaluate, develop and modernize crime Records Bureaux

H. Executive and develop computer-based systems for the Central Police Organisations - and also cater to their data processing and training needs for computerization.

I. To function as the National storehouse of fingerprint (FP) records of convicted persons including FP records of foreign criminals.

J. To help trace interstate criminals by fingerprint search.

K. To advise Central and State Governments on matters related to fingerprints and footprints, and to conduct training courses for finger print experts.

5. CYBER CRIME ANALYSIS

IT Act cases in metro cities. As per the NCRB data of 2016, following analysis can be done.

A. Top 10 Cyber Crime Cities of India

As per NCRB data of 2016 following is the ranking with Vishakhapatnam at the top.

Ranking	City
1	Vishakhapatnam (A.P.)
2	Aurangabad (Maharashtra)
3	Allahabad (U.P.)
4	Vijayawada (A.P.)
5	Varanasi (U.P.)
6	Agra (U.P.)
7	Jodhpur (Rajasthan)
8	Vasai Vihar (Maharashtra)
9	Vadodara (Gujarat)
10	Meerut (U.P.)

B. Top Motives behind the crime

As per the NCRB data of 2016 following is the deduction.

Rank	Motive	City Ranking within the motive
1	Illegal Gain	1. Vishakhapatnam (A.P.) 2. Vijayavada (A.P.) 3. Varanasi (U.P.) 4. Meerut (U.P.) 5. Vadodra (Gujarat)
2	Others (not included in 1 & 3-6)	1. Vishakhapatnam (A.P.) 2. Aurangabad. 3. Jodhpur
3	Extortion/ Black Mailing	1. Allahabad. 2. Agra 3. Vishakhapatnam (A.P.)
4	Sexual Exploitation	1. Vadodara 2. Vasai Vihar.
5	Insult to the modesty of a woman	1. Vijay vada 2. Vishakhapatnam (A.P.)
6	Revenge	1. Agra (maximum)

C. Types of Offenses

As per the legislation crimes may fall under IT Act, under IPC or under SLL. The total cybercrime cases reported in 2016 as per NCRB data was 1370. Out of which 929 were under IT Act, 414 under IPC and remaining 27 under Special and Local Laws (SLL). The further breakdown is enumerated below.

Rank	Legislation type/ No of cases	Sub ranking / No. of cases
1	Under IT Act - 929 cases	1. Computer related offence under Section 66& Sec -66 B to-E . (756) 2. Under Section 66 (365) 3 Under Secton 66C (214) 4. Under section 66D (132) 5. publication/ transmission of obscene/ sexually explicit content etc in electronic form (108) 6. under Section 67A (104)
2	Under IPC – 414 cases	1. Cheating under sec 420 (289) 2. Other IPC crimes (106) 3. Forgery sec 465,468,471 & 477A (9) 3. Data theft (06) 3. Criminal breach of trust / fraud under section 406,408,409 (04)
3	Under SLL (includes Copyright Act, Trade Marks Act 1999) – 27 cases	1. Copyright Act (27) no case reported in Trade Marks and any other SLL)
Total	1370 cases	

6. CONCLUSION

The paper discussed various Cyber Offences under the IT and other acts and made an analysis on the Cybercrime in India using the E-Governance system used by NCRB. NCRB has successfully used the ICT to make available cybercrime and other data successfully to its various users. The data clearly depicts certain states to be reporting a maximum number of cybercrime cases. As per the data, Vishakhapatnam (A.P.) reported the maximum number of cyber offense in 2016. The maximum number of cases were registered under section 66, 66B, 66C, 66D and 66E which falls under computer-related offenses of the IT act 2000. Nil case has been reported so far on Cyber Terrorism. Apart from offenses under IT Act 2000, a maximum number of cases were under section 420 of IPC.

7. REFERENCES

[1] IT Act 2000
[2] NCRB website http://ncrb.gov.in/.
3. Government notification on NCRB

