Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

A COMPREHENSIVE STUDY OF CYBER SECURITY AND E- SURVEILLANCE

Sumiksha Tickoo (Razdan)
Lecturer, Dogra Law College, Jammu

***Abstract*-- As a saying in criminology goes – "a crime will happen where and only when the opportunity avails itself." Until recently, we were aware of only traditional types of crimes like murder, rape, theft, extortion, robbery, dacoits etc. But now with the development and advancement of science and technology there came into existence machines like computers and facilities like internet. The internet has opened up a whole new virtual heaven for the people good and bad, clever and naive to enter and interact with lot of diverse cultures and sub-cultures, geography and demographics being no bar. The very same virtues of internet when gone in wrong hands or when exploited by people with dirty minds and malicious intentions, make it a virtual hell. Stories of copyright theft, hacking and cracking, virus attacks and plain hoaxes etc. have mounted up in the last few years. As a result of the rapid adoption of the internet globally, computer crimes are multiplying like mushrooms. The law enforcement officials have been paralyzed by the inability of the legislators to keep cyber-crime legislation ahead of the fast moving technological curve and due to insufficient technical training. At the same time, the legislators face the need to balance the competing interests between individual rights such as privacy and free speech, and the need to protect the integrity of the world's public and private networks.**

I. INTRODUCTION

'Cyberspace' is the progeny of convergence of computer network and telecommunications facilitated by the digital technologies, Internet is increasingly being used for communication, commerce, advertising, banking, education, research and entertainment. The growing importance of Information Technology can be visualized from the fact that in India for the first time a Delhi based businessman has made a digital will of the secret information saved in his e-mail account. Digital will is a foreign concept which is gaining momentum in India also.[1]The 'cyber man than' has bestowed many gifts to humanity but they come with unexpected pitfalls. It has become a place to do all sort of activities which are prohibited by law like - pornography, gambling, trafficking in human organs and prohibited drugs, hacking, infringing copyright, terrorism, violating individual privacy, money laundering, fraud, software piracy and corporate espionage, to name a few.[2] This new medium which has suddenly confronted humanity does not distinguish between good and evil, between national and international, between just and unjust, but it only provides a platform for the activities which take place in human society. Law as the regulator of human behavior has made an entry into the cyberspace and is trying to cope with its manifold challenges.[3]A legal framework for the cyber world was conceived in India in the form of E-Commerce Act, 1998. Afterwards, the basic law for the cyberspace transactions in India has emerged in the form of the Information Technology Act, 2000 which was amended in the year 2008. The IT Act amends some of the provisions of our existing laws i.e. the Indian Penal Code, 1860; the Indian Evidence Act, 1872; the Bankers Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934.

II. STATUTORY PROVISIONS IN INDIA

In the knowledge society of 21st century, computer, internet and ICT or e-revolution has changed the life style of the people. Apart from positive side of e-revolution there is seamy side also as computer; internet and ICT in the hands of criminals has become weapon of offence. Accordingly a new branch of jurisprudence emerged to tackle the problems of cyber-crimes in cyber space i.e. Cyber Law or Cyber Space Law or Information Technology Law or Internet Law.[4]For the first time, a Model Law on E-commerce was adopted in 1996 by United Nations Commission on International Trade and Law (UNCITRAL). It was further adopted by the General Assembly of the United Nations by passing a resolution on 31st January, 1997. Further, India was also

[1]Ab E-mail Accounts Ki BhiHuiWasiyat", Navbharat Times, 2018
[2]Byte Replaces Bullets On Cyberspace", Hindustan Times, September 18, 2018
[3]Justice T. Ch. Surya Rao, "Cyber Laws – Challenges for the 21st Century", Andhra Law Times,
[4]Justice A.S. Anand, "Cyber Law Needed to Meet IT Challenge", The Tribune,

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

a signatory to this Model Law and had to revise its national laws as per the said model law. Therefore, India enacted the Information Technology Act, 2000 and it was recently amended by the Information Technology (Amendment) Act, 2008.

III. Aims And Objectives Of Information Technology Act, 2000

1. To suitably amend existing laws in India to facilitate e-commerce.
2. To provide legal recognition of electronic records and digital signatures.
3. To provide legal recognition to the transactions carried out by means of Electronic Data Interchange (EDI) and other means of electronic communication.
4. To provide legal recognition to business contacts and creation of rights and obligations through electronic media.
5. To establish a regulatory body to supervise the certifying authorities issuing digital signature certificates.
6. To create civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions.
7. To facilitate e-governance and to encourage the use and acceptance of electronic records and digital signatures in government offices and agencies. This would also make the citizen-government interaction more hassle free.
8. To make consequential amendments in the Indian Penal Code, 1860 and the Indian Evidence Act, 1872 to provide for necessary changes in the various provisions which deal with offences relating to documents and paper based transactions.
9. To amend the Reserve Bank of India Act, 1934 so as to facilitate electronic fund transfers between the financial institutions.
10. To amend the Banker's Books Evidence Act, 1891 so as to give legal sanctity for books of accounts maintained in the electronic form by the banks.
11. To make law in tune with Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) adopted by the General Assembly of the United Nations.[5]

Information Technology (Amendment) Act, 2008-Major Amendments are as follows-Section 3A was inserted into the IT Act which allows for other means of authenticating electronic records. The IT Act also made a number of amendments to the Indian Evidence Actso as to enable production of electronic records as evidence in courtroom proceedings. The most important of these amendments -

Section 3 of the Indian Evidence Act, the term "evidence" now includes "electronic records". Section 47A has been inserted which provides: "Opinion as to digital signature when relevant.- When the court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the digital signature Certificate is a relevant fact".

Sections 65A and 65B have been added which provide as follows: "65A Special provisions as to evidence relating to electronic record." "65B Admissibility of electronic records."

Section 67A has been inserted which provides: "Proof as to digital signature.- Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved."

Section 73A has been inserted which provides, "Proof as to verification of digital signature."

Section 81A has been inserted which provides, "Presumption as to Gazettes in electronic forms"

Section 85A- Presumption as to electronic agreements.

Section 85B- Presumption as to electronic records and digital signatures.

Section 88A- Presumption as to electronic messages.

Section 90A- Presumption as to electronic records five years old.

Section 131 has been substituted with the new section 131 as provided below: "Production of documents or electronic records which another person, having possession, could refuse to produce.- No one shall be compelled to produce documents in his possession or electronic records under his control, which any other

[5]PawanDuggal, Cyber Law – An Overview", available at http://www.cyberlawindia.com. January 2019

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

person would be entitled to refuse to produce if they were in his possessions or control, unless such last-mentioned person consents to their production."
These changes in the Indian Evidence Act have been made to provide a legal regime for the production of electronic records in legal proceedings in India which provides for acceptance of electronic records as evidence, acceptance of digital signatures, digital messages and agreements, etc.

THE INFORMATION TECHNOLOGY (PROCEDURE AND SAFEGUARDS FOR MONITORING AND COLLECTING TRAFFIC DATA OR INFORMATION) RULES, 2009

The Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 issued under section 69B of the Information Technology Act stipulate that directions for the monitoring and collection of traffic data or information can be issued by an order made by the competent authority for any or all of the following purposes related to cyber security:
forecasting of imminent cyber incidents;
monitoring network application with traffic data or information on computer resource;
Identification and determination of viruses or computer contaminant;
tracking cyber security breaches or cyber security incidents;
tracking computer resource breaching cyber security or spreading virus or computer contaminants;
identifying or tracking any person who has breached, or is suspected of having breached or likely to breach cyber security;
undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources;
accessing stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;
Any other matter relating to cyber security.
According to these Rules, any direction issued by the competent authority should contain reasons for such direction and a copy of such direction should be forwarded to the Review Committee within a period of seven working days. Furthermore, these Rules state that the Review Committee shall meet at least once in two months and record its finding on whether the issued directions are in accordance with the provisions of sub-section (3) of section 69B of the IT Act. If the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue an order for the destruction of the copies, including corresponding electronic record of the monitored or collected traffic data or information.

IV. GLOBAL PERSPECTIVE TO CURB CYBER MENACE

Internet operations being of global nature, they do not recognize any territorial boundaries. This enables the cyber criminals to operate beyond the national geographic limits without being physically present at the scene of crime. The problem of cyber-crimes therefore, calls for greater international support and cooperation. Though much has been done by the United Nations to muster cooperation of member nations to tackle the problem of cyber criminality as a common cause, the response from them has not really been very encouraging excepting that there is general consciousness among the countries that where a cyber-crime involving a foreign country or countries is involved, trans-border assistance and cooperation between the concerned countries is the only viable alternative to prevent and control such crimes.[6]
1. International de droitPonel Conference in Germany (1992) - The Association InternationaleDroitPonel (ADIP) held the collegiums on 'Computer Crime and Other Crimes against Information Technology' in Wartzburg (Germany). Its report stated that only 5% computer crimes were being reported to police.
2. Twenty-Second G-7 Summit on Cyber Crime (1996) - The member nations at the G-7[7]Summit on Anti-terrorism held in Leon (France) in July, 1996 resolved to accelerate mutual consultations and cooperation through appropriate bilateral and multi-lateral meetings on encryption that allows, when necessary, lawful

[6]66th U.N. General Assembly Annual Conference of the Interpol held in New Delhi in October, 1997
[7]The group of G-7 countries consisted of Canada, France, Germany, Italy, Japan, UK and USA

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

government access to data and communications in order to prevent or investigate acts of cyber terrorism while protecting the privacy of legitimate communications.[8]The focus of deliberation was on protection of security of information systems, privacy of personal data and protection of intellectual rights of the people.

3. G-8 High-Tech Crime Working Group (1998)- As a part of the international cooperation programme for combating cyber-crime, a G8[9]Hi- Tech Crime Sub-Group was formed in March, 1998, to provide trans-border access to stored data and assistance in hi-tech crime investigations which involve illegal alteration or distribution of electronic evidence. A G-8 Sub-Group Conference was held in Paris (France) in 1998 in which representatives of industries and consumer groups discussed problems regarding security of the internet affecting industrial and consumer establishments and provide for a safe and secure environment for e-commerce.

4. European Convention on Cyber Crime, Budapest (November 2001) - It was held in Budapest on November 23, 2001. This Convention was held for considering the changes brought about by the digitalization, convergence and continuing globalization of computer networks and the risks these computer networks and electronic information were creating in the form of modes and methods for the perpetration of cyber-crimes.

5. International Conference on E-Security, Cyber Crime and Law (2004) – It was held in Chandigarh (India) on 19-20 February, 2004. The main issues for deliberation in the Conference included- Network security for corporate governance and industrial intrusions, Data and transmission standards and encryption methods needed to be improvised, electronic fund transfer and security of data banking, issues related to computer forensics, preservation of computer evidence, Cyber law, data protection and need for appropriate legislation for the purpose was highlighted by the delegates. The issues like policing the cyberspace, role of judiciary in digital age, network security and law and public participation in prevention of cyber-crimes were also extensively discussed in the conference.

6. ASEAN Regional Forum (2004) - The Association of South East Asian Nations (ASEAN) held a high level ministerial meeting on trans-national crimes in Bangkok (China) on January 8, 2004 recognizing the need for an effective legal cooperation to combat the growing menace of cyber-crime in the south east region of Asia. The statement issued by the ASEAN Regional Forum on July 2006 reiterated its resolve to give a thorough fight against the growing menace of cyber space crime by extending common cooperation in legal and other areas of mutual concern. The theme of the discussion was various issues and challenges involved in the investigation of cyber-crimes and measures to be taken to curb this ever growing evil.[10]

7. Asia Pacific Economic Cooperation (APEC) (2004) - The Conference organized by the members of the Asia Pacific Economic Cooperation (APEC) resolved to work out a comprehensive legal framework for the prevention and control of cyber-crime and for strengthening of cyber security in accordance with the set principles of the international law. In its ministerial meeting held in Santiago (Chile) in November, 2004 it was mutually agreed to strengthen economic cooperation to fight against cyber-crime.

8. Eleventh Congress on Prevention of Crime and Treatment of offenders (2005) - In the Eleventh Congress on Prevention of Crime and Treatment of offenders held in Bangkok on 18-25 April, 2005. It was realized that the existing national laws were inadequate to check the constantly rising graph of cyber-crimes at the international level. Therefore, there was need for bilateral, regional and international cooperation in crime prevention and strengthening of the criminal justice system by the participating nations.[11]

9. Seventh International Conference on Cyber Crime (2007) - The Seventh International Conference on Cyber Crime was held in VigyanBhawan, Delhi (India) on September 12, 2007. The Conference emphasized the need for generating cyber security awareness and evolving effective preventive measures to combat cyber criminality. The focus in the conference was on computer generated terrorist activities and organized crimes through internet which the criminals have found to be a lucrative means to generate huge proceeds of time. It was generally agreed that online child pornography, trafficking in contrabands and e-commerce frauds are showing a rising trend and the acts of vandalism and cheating were increasingly frustrating the e-governance

[8]R.K. Suri& T.N. Chhabra, Cyber Crime, (2018)
[9]G-8 countries are USA, UK, Canada, France, Germany, Italy, Japan and Russia.
[10]Harshwardhan, "Investigation of Computer Crime: Issues and Challenges", Criminal Law Journal,
[11]A.S. Chawla, "Cyber Crime – Investigation and Prevention", The Indian Police Journal,

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

efforts. Therefore, the need of the time demands quick response to the Interpol references and bilateral requests, liberal sharing of forensic technology and more cross-country training exchange programmes besides, timely alert to tackle the cyber-crime menace effectively.[12]

10. International Conference on Terrorism and Organized Crimes (2008) - An International Conference on Terrorism and Organized Crimes was held in Anaheim (USA) on August 25, 2008. It deliberated on problems of international and domestic terrorism, misuse of weapons of mass destruction, organized crime, human smuggling and trafficking, identity theft, online drug trafficking international monetary laundering, e-commerce, cyber frauds and computer forensics. The focus of the conference was on the extensive use of forensics in cyber-crime investigations and involvement of computer experts in the process of investigation.

11. UN Congress on Crime Prevention (April 2010) - It enabled the participating nations to have an opportunity to re-enforce the earlier global responses to the threat of cyber-crime. The member countries resolved to launch a crusade against cyber criminals particularly, the cross-border terrorists and the perpetrators of cyber fraud operating internationally.

V. The Basis Of These Recommendations

The suggestions are said to be based on the recommendations made by the expert committee headed by former LokSabha Secretary General T K Viswanathan. That report recommended the following Amendments to the Code of Criminal Procedure 1973:

It has been noted that law enforcement agencies face several challenges during investigation and prosecution of harmful online conduct due to the dearth of technically trained police personnel, lack of access to expert advice, procedural hurdles in conducting cross jurisdictional investigations, absence of comprehensive data on the crimes reported and the lack of a quick and streamlined procedure for takedown of malicious online content. In an attempt to address some of these issues, the Committee proposes the insertion of two new provisions namely, sections 25B and 25C in the Code of Criminal Procedure 1973 thereby creating the post of a State Cyber Crime Coordinator and establishing a District Cyber Crime Cell, respectively. The details pertaining to the State Cyber Crime Coordinator vis-à-vis his qualifications, appointment and functions along with the role, composition and conditions of service of the members of the District Cyber Crime Cell respectively, have been mentioned in these sections. The goal of these provisions is to create a cadre of trained cyber experts, both from within the police force and experts in the fields of information technology, digital forensics, cyber law, etc. to ensure the effective investigation and management of cyber offences.

VI. State Cyber Crime Coordinators

"25B (1) The State Government shall appoint an officer not below, or equivalent to, the rank of an Inspector General of Police, who shall be the Cyber Crime Coordinator of the State.

(2) The functions of the State Cyber Crime Coordinator shall be to:

oversee the functioning of the District Cyber Crime Cells in the State; recommend to the State Government the procedures and best practices to be adopted by the police officers under Section 78 of the Information Technology Act, 2000 and the District Cyber Crime Cells while investigating any offence under the Information Technology Act 2000or involving computer and electronic media under the Indian Penal Code, 1860 or any other law; oversee the training of police officers and experts in the District Cyber Crime Cells in the State; coordinate with the State Cyber Crime Coordinators of other States in case of offences under this Act that fall under the jurisdiction of two or more States; and carry out such other functions as may be specified by the State Government."

VII. District Cyber Crime Cells

"25C (1) The State Government shall establish a District Cyber Crime Cell in every district to assist in the investigation of offences –under the Information Technology Act, 2000; and involving computer and electronic media under the Indian Penal Code, 1860 or any other law.

[12] Global anti-crime Centre mooted at Interpol Conference", The Tribune,

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

(2) The District Cyber Crime Cell shall consist of an officer not below, or equivalent to, the rank of Deputy Superintendent of Police, who shall be the head of the District Cyber Crime Cell;such number of Sub-Inspectors as the State Government may deem fit; and at least three experts in information technology, mobile telephony, digital forensics, cyber law or such other experts with such qualifications to be appointed by the State Government inaccordance with the rules made under subsection (4).
(3) The head of the District Cyber Crime Cell shall report to the State Cyber Crime Coordinator of the State through his supervisory officers.
(4) The State Government shall prescribe by rules –the manner of appointment and the terms and conditions of service or empanelment of the members of the District Cyber Crime Cells under sub section (2); qualifications of experts under clause (c) of sub section (2)."
Departments working under Indian government for surveillancerecently, many departments and agencies have been established, under government of India, in order to do surveillance in cyberspace, these are as follows-

VIII. National Intelligence Grid

National Intelligence Grid aims at linking information saved on servers and networks of different departments and ministries of government so it can be accessible by any department and intelligence agency.[13]National Intelligence Grid does not aim at storing any type of information in its own and will only provide a platform where communication between computers and networks of different departments can be taken place.

IX. Crime and Criminal Tracking Network System (CCTNS)

Crime and Criminal Tracking Network System aims at collecting, storing, analyzing, transferring, sharing of data between various police stations and with State Headquarters and police organizations.[14] By using CCTNS, any police station will get complete available information on any criminal or any suspect stored on the servers of other police stations or departments.

X. Central Monitoring System

Central Monitoring System aims at monitoring every byte of communication i.e. text messages, phone calls, online activities, social media conversations and contents etc. CMS was prepared by the Telecom Enforcement, Resource Monitoring (TERM) and by the Center for Development of Telematics (CDoT) and managed by Intelligence Bureau[15].Today government is doing surveillance on Facebook and Twitter walls by using Central Monitoring System.

XI. Unique Identification Authority of India (UID Scheme)

Unique Identification Authority of India (UID scheme)aims at providing a special unique identity to every citizen of India in which figure print and basic information of a person. Scheme comes under AADHAAR Scheme of government of India.

XII. Indian Computer Emergency Response Team (CERT-In)

CERT, functional since January 2004, is a nodal agency of government in response of any computer security incident. CERT has been created under the provisions of Information Technology Amendment Act, 2008 and since then working as government agency[15]. CERT is not exactly surveillance agency of government but it is response team of government in order deal with any cyber security incident all over India.

XIII. National Counter Terrorism Center (NCTC)

After the attacks on Mumbai in 2008 aka 26/11 attacks on Mumbai, there was a need of agency to fight against terrorism as there was a failure on the part of intelligence agencies in India. So the proposal of NCTC was

[13]PTLB, National Intelligence Grid (NATGRID) project of India,
[14]B. S. Dalal, Indian Center for Communication Security Research and Monitoring (CCSRM),
[15]Maria Xynou, India's Big Brother: Central Monitoring System,

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

made. NCTC will derive its powers from Unlawful Activities Prevention Act, 1967 and it will be part of Intelligence Bureau headed by the director.

XIV. CYBER POLICING IN INDIA

Crime and Criminal Tracking Network and Systems (CCTNS)

Approved by the Cabinet Committee on Economic Affairs in 2009, with an allocation of INR 2 billion, the CCTNS is a project under the National e-Governance Plan. It aims at creating a nationwide networking infrastructure for an IT-enabled criminal tracking and crime detection system. The integration of about 15,000 police stations, district and state police headquarters and automated services was originally scheduled to be completed by 2012. However, this still remains incomplete. Apart from the slow pace of implementation and budgetary problems, on-the-ground hurdles to fully operationalizing CCTNS include unreliable Internet connectivity and under-trained personnel at police stations. Other issues include unavailability of facilities for cyber forensic analysis in most locations, and lack of awareness regarding online citizens' services such as verification of tenants and employees and clearance for processions and events.

Online Complaints

The Central Government, in response to queries by the Supreme Court regarding measures taken to tackle cybercrime, recently announced that they would be setting up a 'Centre Citizen Portal'. This portal will allow citizens to file complaints online with respect to cybercrimes, including cyber stalking, online financial fraud and others, suffered or observed by them. The governmental response also details the proposed process, stating that any such complaint on the portal will trigger an alert at the relevant police station and allow the police department to track and update its status, while the complainant too would be able to view updates and escalate the complaint to higher officials.

Cyber Police Stations

Cyber police stations generally include trained personnel as well as the appropriate equipment to analyze and track digital crimes. Maharashtra, where cyber-crime has risen over 140% in recent times, and which had the dismal distinction of only recording a single conviction related to cybercrime last year, is converting its existing cybercrime labs into cyber police stations. This will mean there is a cyber-police station in each district of the state. The initiative in Maharashtra is useful especially because of the rise in online transactions in Tier II and Tier III cities and the rising cybercrime related thereto. However, despite the rise in cybercrime, complaints remain of low reportage and low success rates in solving crime. Police officers point to problems processing evidence, with complex procedures being required to retrieve data on servers stored abroad.

Predictive Policing

Predictive policing involves the usage of data mining, statistical modeling and machine learning on datasets relating to crimes to make predictions about likely locations for police intervention. Examples of predictive policing include hot-spot mapping to identify temporal and spatial hotspots of criminal activity and regression models based on correlations between earlier, relatively minor, crimes and later, violent offences. In 2013, the Jharkhand Police, in collaboration with the National Informatics Centre, began developing data mining software for scanning online records to study crime trends. The Jharkhand Police has also been exploring business analytics skills and resources at IIM-Ranchi, in order to tackle crime in Jharkhand.

The Delhi Police has tapped into the expertise at the Indian Space Research Organization order to develop a predictive policing tool called CMAPS– Crime Mapping, Analytics and Predictive System. The system identifies crime hotspots by combining Delhi Police's Dial 100 helpline calls data with ISRO's satellite imagery and visualizing it as cluster maps. Using CMAPS, Delhi Police has slashed its analysis time from the 15 days it took with its erstwhile mechanical crime mapping to the three minutes it takes for the system to refresh its database.

The Hyderabad City Police is in the process of building a database, called the 'Integrated People Information Hub' which, according to the City Police Commissioner, would offer the police a "360-degree view" of citizens, including names, aliases, family details, addresses and information on various documents including passports, Aadhaar cards and driving licenses. The data is combed from a wide-ranging variety of sources, including information on arrested persons, offenders' list, FIRs, phone and electricity connections, tax returns,

Indexed with IIJIF
Impact Factor : 1.021
ISSN: 2456 - 608X
International Journal of Legal Research and Studies
A Peer-Reviewed Refereed Online Law Journal

RTA registrations and e-challans. It is further indexed with unique identifiers, and is used to establish the true identity of a person, and present results to relevant authorities within minutes.

XV. DRAWBACKS OF THE INFORMATION TECHNOLOGY ACT, 2000

Information technology has played very important role in the lives of people. Despite the various advantages, the Information Technology Act, 2000 has the following drawbacks:

I. Jurisdiction- Cyber jurisdiction refers to a real world government's power and a normally existing court's authority over internet users and their activities in the cyber world. However, the IT Act does not cover the important issue of jurisdiction which is very important legal aspect in deciding the place of filing the case.

II. E-mail authenticity or its evidentiary value- IT Act does not touch e-mail authenticity or its evidentiary value in the hands of receiver.

III. Domain name infringement- The concept of e-commerce is mainly based upon domain name. However, this Act is silent about the domain names infringement, cyber-squatting, typo squatting, spamming and security of information at various levels.

IV. Cross-border tax- In the era of globalization, international trade and taxation policies are very important. However, this Act does not talk about the cross-border taxation policy at the international level when the international contract is signed online.

V. Failure to surrender license is a non-cognizable offence- According to section 33 of the IT Act, 2000 when license of the certifying authority is suspended or revoked then he must immediately surrender his license to controller. However, where such certifying authority fails to surrender license then he shall be guilty of an offence and shall be punished with imprisonment which may extend up to 6 months or a fine which may extend to Rs. 10,000 or both. Further, u/s 77B, which is incorporated by the IT (Amendment) Act, 2008 any offence punishable with imprisonment of 3 years or above shall be cognizable. Therefore, failure to surrender license u/s 33 is a non-cognizable offence. However, license is backbone of digital/electronic signature certificates because only licensed CA can issue digital/electronic signature certificates, therefore, where a CA whose license has been revoked or suspended if fails to surrender his license then it should be a cognizable offence.

VI. The term cyber-crime and cyber offence as such is not defined under IT Act, 2000.

VII. Important documents such as power of attorney etc. are not covered.

VIII. Statutory bodies may not accept electronic documents- On one hand, the main aim and objective of the IT Act, 2000 was to facilitate e-governance, however on the other hand, section 9 provides that no one can insist any government office to interact in electronic form.

CONCLUSION

Indian's growing legislative framework and surveillance policies are not adequate to deal with future threats and there is an urgent need to amend existing legal framework as well as to introduce strong and effective policies in order to protect IT industry as well as to protect privacy of individuals in the country. As referred above, UK, US and China have very effective policies and the workings of agencies as well as the laws relating to surveillance and privacy of its citizens. Similarly, in India, legislature should pass such acts and rules in relation to working of agencies, powers and authorities under whom surveillance will be done, protection and destruction of such data collected during surveillance and how far the privacy of individual is secured.