International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 10-12-2020; Accepted: 24-12-2020; Published: 12-01-2021
www.lawjournals.org
Volume 7; Issue 1; 2021; Page No. 26-29

Information technology act, 2000: an introduction of cyber security provision in India-a study

Aishwarya Pramod Athawale
Advocate, Department of Bhusawal Court, Dr Ulhas Patil Law College, Kavayitri Bahinabai Chaudhari North Maharastra University Jalgaon, Maharashtra, India

Abstract
Computer, an electronic device performs multitude of dimensional functions, it is a handy instrument of assessing information which ameliorate access to detail with the help of connected network system, Computer technology has its concrete foundations based on knowledge, and have strong footing in present civilization, which serves as a comprehensive source of copious fact and details globally. But infelicitously computing is also used as an instrument to carry out illicit activities.

Keywords: cyberspace, cybercrime, cyber security

Introduction
Computers integrated with network need protocol Suite to access the internet and connect to other computers and most significant outcome of inventing computer is probably the information and commination technology, cohering the world and it definitely favours Illusion of progress, which is a Paramount source of knowledge captivating towards progression. Also it has a substantial impact on lives of people through direct and indirect contribution to the various social economic parameter. The term cyber is the most important characteristic of Information Technology related to the virtual world of Computer. Computing without doubt is crucial for advancement as well as it has a numerous benefit brought by technology advancement apart from this it has also became a device in the hand of perpetrator to commit illegal function which has misleaded the true purpose of inventing Computer technology [1].

Cyber Space
Cyberspace is described as computer simulated place or environment constructing worldwide interaction between people by Information and Communication Technology helping people to communicate, interact, exchange thoughts and ideas and a convenient tool to share information. According to Gibson cyberspace is the name of a real non-space world which is characterised by the ability of virtual presence and serve as a common pool of interaction between people having many folds of network and devices making it more complex to draw clear boundaries among the different groups to deter unlawful act from cyberspace. The cyber world is swiftly enlarging and the computer network has been immensely used worldwide allowing the user to carry out multitude of function. The multifaceted uses of present technology has often lead to many vulnerable incident in the realm of cyberspace exploiting the security and authenticity of Information and Communication Technology [2].

Cyber crime
Cybercrime is a ramified act of a perpetrator using computer Technology as a medium to commit offence. it is a concoction of illegal acts committed using computer networks to corrupt and copy data or software without proper authority, an unauthorised and uncredited access within the privacy of user without his sanction, these Erroneous act are certainly forbidden and refers to a legal concept, can be defined as an unlawful act where computing is the source to commit crime. Cybercrimes are extremely uncomplicated to carry out in exceptionally (compact) less expedient and certainly has flared the commission of such unwelcome incidents with an atmosphere ease but vernalisation caused due to Cyber-attacks could be very immense.
Cybercrime can be committed against person, property or against government some of the example of cyber threat to individuals are breach of confidence and privacy, social engineering, cyber defamation, hacking or hacktivism, cyber bullying, cyber staking and harassment, pornography, Cyber-attacks against property of intellectual possession include data leakage or data diddling, theft of information-commerce investment fraud, theft of information contained in electronic form. Cyber terrorism, attack on computer through virus, worms or by malicious software code are also committed, these crimes are an organised attacks which not only threatens life of people but also has an adverse effect on economy and quenches national security [3].
Government has made significant effort and is continuously striving hard to secure cyberspace and has enacted many laws and provision to secure cyber activities carried through the Information and Communication Technology.

Information Technology Act, 2000
Information Technology Act, 2000 is the primary law in India dealing with cybercrime. It was formulated to prevent, investigate and prosecute computer crime by working to improve the excess of its use, which also include meticulous monitoring on the web traffics. Enactment of this act has provided a legal recognition for transaction carried out by business of e-commerce, retributing the act of tempering with computer sources or document, hacking computer system, publishing obscene information, unauthorised access to protected system, breach of confidentiality and privacy, for publishing false digital signature and certificates [4].
Information Technology Act,2000 was further amended in

2008 to bolster confidence in transaction carried out by electronic means by providing legal recognition, Indian penal code 1860, Indian evidence act 1877, banker's book act,1891, Reserve bank of India act 1934 were also amended to derail cybercrime.
The laws amended to prevent cybercrime and related threats to it [5]:-

Indian penal code 1860
Provisions in Indian Penal Code are coherently used to penalised criminal activities carries on cyber space, infringing the constitutional rights guaranteed to people such as defamation, sending threatening message by email, forgery of electronic record, bogus website, cyber frauds, emails scooping, web jacking, and abusing through email which pernicious the use of youth against the interest of general public.

Indian Evidence Act, 1877
The Indian evidence act was amended within the purview of information technology act, 2000, which gave recognition to all form of electronic documents, under sec 65(B) it got significance for admissibility of electronic record.

Bankers Book Evidence (BBE) Act, 1891
To prevent unauthorised change or misuse of data, security system was adopted by amending BBE act, 1891 to ensure data entered through the electronic medium must be performed by authorised person to form a valid document, which cannot be manipulated or accesses in an unauthorised manner.

Reserve Bank of India (RBI) Act 1934
Use of information technology by banks was growing speedily and thus formed an important part of the operational strategy of bank, numerous cases of Cyber-attack incident had also been increased in financial sectors including Banks.
Therefore, to ensure adequate security for the assessment and to enable enhanced security from cyber threat section 58 (2) clause (p) was inserted under this act, to help improve the current defences addressing cyberattack relating to electronic transfer and to immediately put in place cyber security policy to ensure legal admissibility of electronic documents and records.

Provision for Cyber Security in India
Cyberspace has definite standards, rules and regulation to follow known as Cyber Law, encompassing laws related to information and communication technology, transgression of this Ordinance lead to commission of cybercrime which include many aspects of intellectual property and technology transfer. Separate body of law and legal code of system was formulated to tackle the issue of Cybercrime. Existing laws were amended in India to stipulate numerous provision for cyber security with an aim to secure Electronic Commerce and information technology [6].
To avert cyber threat depending on the level of complexity of business relating to online transaction including authenticity of digital signature and E-certificates and for imposing liability for data breaches. Many rules and regulation was framed within the ambit of information technology act, 2000 to prevent cybercrime.
Hence the following laws were moduled under Information Technology Act, 2000 to better access cyber security [7]

Information Technology Act, 2000 (Procedure and Safeguards for Interception, Monetary and Decryption of Information) Rules, 2009
Formation of these rules mandates that, no person shall carry out The intersection of monetary or description of any information generated, transmitted, received or stored in any computer resource without prior permission of authorities or by an order issued by the competent authority and the information must be used with utmost security. it was crucial under the said rule that, every intermediary authorities shall designate at least one person to receive and handle the direction for blocking of access by the public about any information generated transmitted and received and stored or hosted in any computer resource which is harmful or offensive in nature, according to the provision given in IT Act, 2000 under sub section 1 of 69(a) [8].

Information Technology Act, 2000 (Intermediary Guidelines) Rules, 2011 [9]
The intermediaries guidelines are made to secure violation of section 3 under IT Act, 2000 and established rules, regulation, privacy policies and user agreement for excess of intermediaries to proper usage of computer resources by any person with the necessary term and condition or user agreement to inform the user of computer resources, about the content and prohibits any such contain to host, display, upload, modify, publish, transmit, update or share any information that belongs to another person to which the user does not have any right to do so or the contents violates any law for the time being in force, which is grossly harmful, offensive, menacing in nature, impersonating others, Infringing any patent Trademark copyright or other privacy.

Reasonable Security Practice and Procedure and Sensitive Personal Data or Information Rules, 2011 (SPDI)
Which says information must be collected only if it is essential and required for lawful purpose. Also it makes it vital to ensure that the person providing necessary information has knowledge about collection and purpose of provided information, it is crucial for the authority to maintain and follow the adequate privacy policy to secure the collected information and for not maintaining reasonable security practices and procedure in relation to sensitive personal data or information, provision is bequeathed in the given rules under sec 43(a) and 72 (a) of IT Act,2000 to recompense for negligent act.

Information Technology Act, 2000 (Indian Computer Emergency Response Team) CERT, 2013
To better response cyber security and to avoid most frequent incidents such as identity theft, intrusion into computer resources, defacement of websites, etc. CERT was formulated within the ambit of information technology act, 2000 to effectively control these illicit activities of Cybercrime occurring in the computer resource [10].

Implementation of Section 66 (a) of Information Technology Act, 2013- The advisory grants power to arrest a person for posting allegedly offensive content on website with prior approval from competent authorities for such arrest, certain incident reported under section 66 (a) of IT

Act,2000 were on upsurge and this act has been invoked slowly with the section of Indian penal code,1860 against posting certain contents which was considered harmful, Supreme Court declared 66(a) of IT Act, 2000 as unconstitutional and struked it down, and allowed the government to block website if the contents had the potential to create disorder.

National Cyber Security Policy, 2013

Ministry of communication and information technology released the national Cyber security policy 2013, to protect the public and private infrastructure from cyber-attack, creating secure computing environment, to provide adequate policy to gain confidence and trust of users in electronic transactions, software service devices and network with a suitable cybersecurity ecosystem in country to tune with Global network environment to build a secure and resilient cyberspace for citizen, business and for government.

Information Technology, Act 2000, (Information Security Practices and Procedure for Protected System) Rules, 2018

It is a detailed infrastructure system to protect cyber threat and to implement cyber security practices as well as it endeavours certain protective measures required to be taken towards securing sensitive Collection of data.

Secure Electronic Record and Digital Signature

Section 14 to 16 of IT Act, 2000 has been made to ensure authentic electronic record and signature, the information contained in the smart card or in Hardware token as the case may be in solely under the control the person who is permitted to have created the digital signature. the digital signature can be verified by using the public key listed in the digital signature certificate issued to the person, which makes it necessary to have security policies relating to the creation, storage, transmission of digital signature, intended in electronic record in such manner that if the electronic record was altered the digital signature would be invalidated.

Department of Telecommunication (DOI) and Security Exchange Broad of India (SEBI)

It is a cyber-resilience framework to address, Identify, protect, detect, respond and recover the cyber threat. since 1992 the securities and exchange Board of India has sought to focus on securing system as part of the operational risk management framework, to secure the interest of investor, securing the networks and Database from cyber-attacks, ensuring that Indian capital market works in systematic manner by formulating comprehensive cyber security to access and manage cyber security risks associated with thereto.

National Critical Information Infrastructure Protection Centre (NCIIPC)

An organisation of Government of India created under section 70 of Information Technology Act amended in 2008 as a national nodal agency in respect of critical information infrastructure protection, to facilitate safe, secure, and resilient information infrastructure for critical sector of nation to take all necessary measures to enhance protection of data from unauthorised access, modification, use, disclosure, description, incapacitation, or from distraction through coherent coordination, because security awareness among all stakeholders is also crucial to better response cyber-attacks.

Conclusion

Cyber security in India has several Central bodies that deal with cyber issues and each has a different reporting structure. John w bagby said after emergency of Computer technology various new concepts such as E- commerce, E-government, E- contract, E- transaction, Intellectual Property Rights in digital medium etc. is discovered and soon information technology and telecommunication has been enormously used for multitude purpose. to one side Information Technology has unequivocal use of E - Revolution but it also has sordid side, where computer has become deep pocket for perpetrators to commit crimes. Cyber security breaches are more contemptuously committed where an unauthorised acquisition of an entity or data of information that compromises the confidentiality integrity availability of information maintained in computer resources. progress in based on the use of tool and telecommunication in the country in which it is used but progress and advancement cannot be claimed to achieve unless cyber-attacks and threats on the technology does not get completely ravished. the legal system which is in place for cyber security needs to effectively import the laws made to curb Cyber threats India.

References

1. Cyber laws and information technology by Dr.Jyoti Rattan -5th edition, 2015.
2. Meaning of cyberspace, author Vassilys Fourkas March, 2004.
3. Cyber Law Simplified Vivek Sood -Tata McGraw-Hill Education - Computer crime, 2001.
4. The Information Technology ACT, 2008. Ministry of Law, Justice and Company Affairs (Legislative Department) New Delhi, the /Jyaistha. 2000; 19:1922.
5. Cyber Law in India Kindle Edition by Talat Fatima.
6. Cyber Law in India the information technology act 2000, 06 2001 by Pavan Duggal Cyberlaws.
7. Ministry Of Communication and Information Technology. National Cyber Security. Policy Department of Electronics and Information, 2013.
8. Information Technology Act 2000Notification under IT(Amendment) Act, 2008,IT (Amendment) Act 2008 2.29 MB,IT Act 2000,Rules for the Information Technology Act 2000,Report of the Expert Committee on Amendments to IT Act 2000
9. Computer crime and intellectual property section,the United States department of Justice John Lynch Chief, Computer Crime & Intellectual Property & prosecuting intellectual property crime fourth editon Published by Office of Legal Education Executive Office for United States Attorneys See United States v. Caceres, 440 U.S, 1979, 741
10. The Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018- Published vide Notification No. S.O. 2235(E), dated 22nd May, 2018.
11. Ministry of Electronics and Information Technology Government of India.
12. Indian Computer Emergency Response Team official Ministry of Electronics and Information Technology

Government of India Since, 2004.
13. Cyber laws in India, legal aspect book, Source: Book on “IT” Security of IIBF Published by M/s TaxMann Publishers.
14. Cyber security in India, AZB and partners, India, 2020.
15. Protection of Information and the Right to Privacy - A New Equilibrium? Editors: Floridi, Luciano (Ed.), 2014.
16. Importance of cyber law in India by Vinitverma K.R. Mangalam University, legalserviceindia.com.